SISTEM PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE NIST SP 800-30 (STUDI KASUS : SISTEM AKADEMIK UIN SUSKA RIAU)

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Teknik pada
Jurusan Teknik Informatika
Oleh:

MELATI SUKMA DEWI
11451201860

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2019

LEMBAR PERSETUJUAN

SISTEM PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE NIST SP 800-30

(STUDI KASUS: SISTEM AKADEMIK UIN SUSKA RIAU)

TUGAS AKHIR

oleh

MELATI SUKMA DEWI
11451201860

Telah diperiksa dan disetujui sebagai laporan tugas akhir di Pekanbaru pada tanggal 30 Desember 2019

Pembimbing I

Reski Mai Candra, S.T., M.Sc.
NIP. 19860505 201503 1 006

LEMBAR PENGESAHAN

SISTEM PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE NIST SP 800-30

(STUDI KASUS: SISTEM AKADEMIK UIN SUSKA RIAU)

TUGAS AKHIR

Oleh

MELATI SUKMA DEWI

11451201860

Telah dipertahankan di depan sidang dewan penguji

Sebagai salah satu syarat untuk memperoleh gelar sarjana Teknik Informatika

Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau

di Pekanbaru, pada tanggal 30 Desember 2019

Pekanbaru, 30 Januari 2019

Mengesahkan,

Dekan,	**Ketua Jurusan,**
Dr. Ahmad Darmawi, M.Ag.	**Dr. Elin Haerani, S.T., M.Kom**
NIP. 19660604 199203 1 004	**NIP. 19810523 200710 2 003**

DEWAN PENGUJI

Ketua	: Novriyanto, S.T., M.Sc.
Sekretaris	: Reski Mai Candra, S.T., M.Sc.
Penguji I	: Muhammad Irsyad, S.T, M.T
Penguji II	: Iwan Iskandar, S.T, M.T

iii

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum dengan ketentuan bahwa hak cipta pada penulis. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan seizin penulis dan harus disertai dengan kebiasaan ilmiah untuk menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh tugas akhir ini harus memperoleh izin dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan yang meminjam tugas akhir ini untuk anggotanya diharapkan untuk mengisi nama, tanda peminjaman dan tanggal pinjam.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan didalam daftar pustaka.

Pekanbaru, 30 Desember 2019

Yang membuat pernyataan,

MELATI SUKMA DEWI

11451201860

LEMBAR PERSEMBAHAN

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Maka nikmat tuhanmu yang manakah
yang kamu dustakan? (QS. Ar-rahman 13)

Assalamu'alaikum Warahmatullahi Wabarakatuh

Ku susun jari jemari ku diatas keyboard laptop ku sebagai pembuka kalimat persembahan. Diikuti dengan Bismillahirrahmanirrahim sebagai awal setiap memulai pekerjaan.

Sebuah langkah telah usai sudah, satu cita-cita telah tercapai. Sembah sujud serta puji dan syukurku pada-Mu Allah SWT. Tuhan semesta alam yang menciptakanku dengan bekal yang begitu teramat sempurna. Taburan cinta, kasih sayang, rahmat dan hidayat-Mu telah memberikan ku kekuatan, kesehatan, semangat pantang menyerah dan memberkatiku dengan ilmu pengetahuan serta cinta yang pasti ada disetiap ummat-Mu. Atas karunia serta kemudahan yang Engkau berikan akhirnya tugas akhir ini dapat terselesaikan. Sholawat dan salam selalu ku limpahkan kepada Rasulullah Muhammad SAW.

Ku persembahkan tugas akhir ini untuk orang tercinta dan tersayang atas kasihnya yang berlimpah yaitu Ayahanda dan ibunda tercinta sebuah tulisan dari didikan kalian yang ku aplikasikan dengan ketikan hingga menjadi barisan tulisan dengan beribu kesatuan, berjuta makna kehidupan, tidak bermaksud yang lain hanya ucapan TERIMA KASIH yang setulusnya tersirat dihati yang ingin ku sampaikan atas segala usaha dan jerih payah pengorbanan untuk anakmu selama ini. Hanya sebuah kado kecil yang dapat ku berikan dari bangku kuliahku yang memiliki sejuta makna, sejuta cerita, sejuta kenangan, pengorbanan, dan perjalanan untuk dapatkan masa depan yang ku inginkan atas restu dan dukungan yang kalian berikan.

Terimakasih untuk do'a - do'anya

Semoga tugas akhir ini bermanfaat bagi pembacanya Allahumma Amin .

SISTEM PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE NIST SP 800-30

(STUDI KASUS: SISTEM AKADEMIK UIN SUSKA RIAU)

MELATI SUKMA DEWI

11451201860

Tanggal Sidang : 30 Desember 2019

Periode Wisuda : November 2020

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRAK

Keamanan informasi merupakan tindakan melindungi informasi terhadap berbagai ancaman demi menjamin kelangsungan proses bisnis yang ada, serta mengurangi risiko. Risiko adalah kejadian yang menyebabkan kerusakan atau kerugian, salah satu cara menangani risiko adalah dengan membuat penilaian risiko. Penilaian risiko merupakan tahapan-tahapan untuk menganalisis atau mendeskripsikan risiko, dan memberikan strategi yang bisa diterapkan untuk meminimalisir risiko. Berdasarkan wawancara yang dilakukan dengan staf divisi aplikasi Pusat Teknologi Informasi dan Pengumpulan Data (PTIPD), sistem akademik pada UIN Suska Riau belum memiliki standar sehingga sistem ini rentan terhadap risiko. Pada tanggal 27 desember 2018 terjadi kebakaran *Uninterruptible Power Supply* (UPS) pada ruangan server, menyebabkan server tidak dapat digunakan dalam waktu lama. Banyak kejadian yang mengakibatkan sistem ini tidak aman, sehingga diperlukan suatu sistem penilaian risiko keamanan informasi untuk mengetahui tingkat risiko pada sistem akademik dan cara mengatasinya. Pada penelitian ini penulis menggunakan metode NIST SP 800-30 untuk melakukan penilaian risiko, metode ini adalah metode yang memberikan panduan manajemen dan penilaian risiko untuk sistem teknologi informasi yang merupakan standar dari pemerintahan *United States*. Hasil dari penilaian menggunakan Sistem Penilaian Risiko Keamanan Informasi menggunakan Metode NIST SP 800-30 terhadap sistem akademik UIN Suska Riau, didapat 5 (lima) risiko level sedang, 4 (empat) risiko level tinggi.

Kata Kunci: Keamanan Informasi, NIST SP 800-30, Penilaian Risiko, Risiko, Sistem Informasi Akademik.

SISTEM PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE NIST SP 800-30

(STUDI KASUS: SISTEM AKADEMIK UIN SUSKA RIAU)

MELATI SUKMA DEWI

11451201860

Tanggal Sidang : 30 Desember 2019

Periode Wisuda : November 2020

Jurusan Teknik Informatika

Fakultas Sains dan Teknologi

Universitas Islam Negeri Sultan Syarif Kasim Riau

ABSTRACT

Information security is an act of protecting information against various threats in order to ensure the continuity of existing business processes, as well as reducing risk. Risk is an event that causes damage or loss, one way to deal with risk is to make a risk assessment. Risk assessment is the stages for analyzing or describing risks, and provides strategies that can be applied to minimize risk. Based on interviews conducted with staff members of the Information Technology and Data Collection Center (PTIPD) application division, the academic system at UIN Suska Riau does not yet have standards so the system is vulnerable to risk. On December 27, 2018 an Uninterruptible Power Supply (UPS) fire broke out in the server room, causing the server to be unusable for a long time. Many events cause this system to be insecure, so an information security risk assessment system is needed to determine the level of risk in the academic system and how to deal with it. In this study the authors used the NIST SP 800-30 method to conduct a risk assessment, this method is a method that provides management guidance and risk assessment for information technology systems that are the standard of the United States government. The results of the assessment using the Information Security Risk Assessment System using the NIST SP 800-30 Method on the UIN Suska Riau academic system, obtained 5 (five) medium level risks, 4 (four) high level risks.

Keywords: Academic Information Systems, Information Security, NIST SP 800-30, Risk Assessment, Risks.

KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْم

Alhamdulillahirabbil'alamin, Puji dan Syukur penulis ucapkan kehadirat Allah SWT karena atas limpahan Rahmat dan Hidayah-Nya lah penulis mampu menyelesaikan Kerja Praktek ini dengan baik. Shalawat serta salam juga untuk nabi kita Nabi Muhammad SAW, karena atas jasa Beliau lah yang telah membawa manusia dari masa kebodohan menuju masa yang penuh ilmu pengetahuan seperti saat ini.

Kesuksesan penulis dalam penyusunan proposal ini tidak lepas dari berbagai pihak yang memberikan dukungan, pengetahuan, bimbingan dan arahan kepada penulis dalam proses penyusunan dan pelaksanaan tugas. Untuk itu pada kesempatan ini penulis ingin megucapkan terima kasih kepada :

1. Kedua Orang Tua yang selalu memberikan dukungan dan men-do'akan segala yang terbaik untuk penulis.
2. Bapak Prof. Dr. KH. Akhmad Mujahidin, M.Ag., selaku Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
3. Bapak Dr. Ahmad Darmawi, M.Ag., selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
4. Ibuk Dr. Elin Haerani, ST, M.Kom., selaku Ketua Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
5. Bapak Muhammad Fikry, ST, M.Sc., selaku Sekretaris Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
6. Iis Afrianti, ST, M.Sc, CIBIA., selaku Koordinator Tugas Akhir Jurusan Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau.
7. Bapak Reski Mai Candra ST, M.Sc., selaku Dosen Pembimbing Tugas Akhir yang selalu bersedia mendengarkan dan memberikan solusi-solusi dalam pembuatan tugas akhir ini.

8. Bapak Muhammad Irsyad, ST, MT., selaku Dosen Penguji I yang bersedia meluangkan waktu untuk memberikan masukan-masukan yang berguna dalam pembuatan tugas akhir ini.
9. Bapak Iwan Iskandar, ST, MT., selaku Dosen Penguji II yang bersedia meluangkan waktu untuk memberikan masukan-masukan yang berguna dalam pembuatan tugas akhir ini.
10. Bapak dan Ibu Dosen dan pengurus Jurusan Teknik Informatika yang tidak bisa disebutkan penulis satu persatu dalam memberikan berupa pengalaman dan ilmu kepada penulis.
11. Keluarga besar TIF A angkatan 2014, yang telah membantu dalam memberikan semangat dan informasi tentang penyusunan Tugas Akhir ini.
12. Adek penulis, (Aldi, Aidil, dan Airin) yang telah membantu penulis dalam memberikan do'a dan semangat kepada penulis sehingga penulis dapat menyelesaikan Tugas Akhir ini.
13. Seluruh keluarga yang selalu mendo'akan dan mendukung penulis dalam menyelesaikan tugas akhir ini.

Semoga Tugas Akhir ini bermanfaat bagi penulis khususnya, atau para pembaca pada umumnya. Penulis berharap bisa mendapatkan masukan dan kritikan yang membangun dari pembaca atas laporan ini, dengan harapan semoga ke depannya penulis mampu memperbaiki kekurangan dan kesalahan yang terdapat didalamnya. Akhir kata penulis ucapkan terima kasih.

wassalamu'alaikum wa rahmatullahi wa barakaatuh

Pekanbaru, April 2018

Penulis

DAFTAR ISI

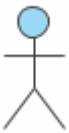
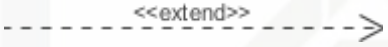
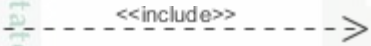
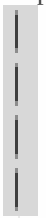
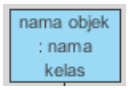
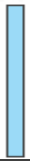
DAFTAR GAMBAR

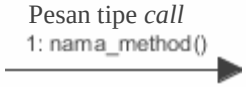
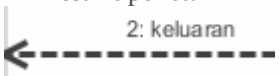
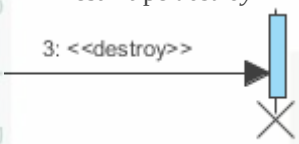
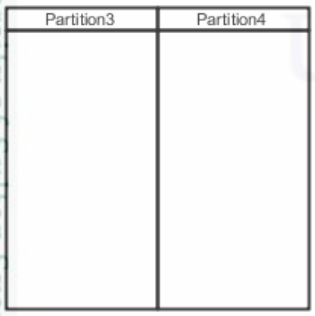
Gambar **Nomor**

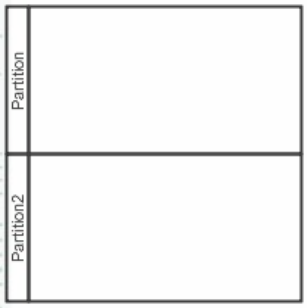
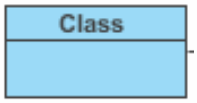
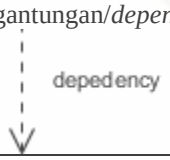
DAFTAR TABEL

Tabel **Nomor**

DAFTAR SIMBOL

Simbol	Deskripsi
Use Case 	merupakan fungsionalitas yang disediakan sistem sebagai unit-unti yang saling bertukar pesan antarunit atau aktor; biasanya dinyatakan dengan menggunakan kata kerja di awal frase nama *use case.*
Aktor 	merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat diluar sistem informasi yang akan dibuat itu sendiri, jadi walaupun *symbol* dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang; biasanya dinyatakan menggunakan kata benda di awal frase nama *actor.*
Asosiasi	Merupakan komunikasiantara actor dan *use case* yang berpartisipasi pada *use case* atau *use case* memiliki interaksi dengan *actor*.
Extensi/*extend* 	Relasi *use case* tambahan ke sebuah *use case* dimana *use case* yang ditambahkan dapat berdiri sendiri walau tanpa *use case* tambahan itu; mirip dengan prinsip *inheritance* pada pemrograman berorientasi objek; biasanya *use case* tambahan memiliki nama depan yang sama dengan *use case* yang ditambahkan.
Generalisasi/*generalization* 	Hubungan generalisasi dan spesialisasi (umum - khusus) antara dua buah *use case* dimana fungsi yang satu adalah fungsi yang lebih umum dari lainnya.
Menggunakan / *include* / *uses* 	Relasi *use case* tambahan ke sebuah *use case* dimana *use case* yang ditambahkan memerlukan *use case* untuk menjalankan fungsinya sebagai syarat dijalankan *use case* ini.
Garis hidup / *lifeline* 	Menyatakan kehidupan suatu objek
Objek 	Menyatakan objek yang berinteraksi pesan
Waktu aktif 	Menyatakan objek dalam keadaan aktif dan berinteraksi pesan

Simbol	Deskripsi
Pesan tipe *call* 	Menyatakan suatu objek memanggil operasi/metode yang ada pada objek lain atau dirinya sendiri
Pesan tipe *send* 	Menyatakan bahwa suatu objek mengirimkan data/masukan/informasi ke objek lainnya, arah panah mengarah pada objek yang dikirimi
Pesan tipe *return* 	Menyatakan bahwa suatu objek yang telah menjalankan suatu operasi atau metode menghasilkan suatu kembalian ke objek tertentu, arah panah mengarah pada objek yang menerima kembalian
Pesan tipe *destroy* 	Menyatakan suatu objek mengkahiri hidup objek yang lain, arah panah mengarah pada objek yang di akhiri, sebaiknya jika ada create maka ada *destroy*
Status Awal 	Merupakan status awal aktivitas *system*, sebuah diagram aktivitas memiliki sebuah status awal
Aktivitas 	Merupakan aktivitas yang dilakukan *system*, aktivitas biasanya diawali dengan kata kerja
Percabangan / *decision* 	Asosiasi percabangan dimana jika ada pilihan aktivitas lebih dari satu
Penggabungan / *join* 	Merupakan asosiasi penggabungan dimana lebih dari satu aktivitas digabungkan menjadi satu
Status Akhir 	Status akhir yang dilkaukan oleh system, sebuah diagram aktivitas memiliki sebuah status akhir
Swimlane Vertikal  Atau	Memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang terjadi

Simbol	Deskripsi
Horizontal 	
Kelas 	Merupakan kelas pada struktur *system*.
Asosiasi/*association*	Merupakan relasi antar kelas dengan makna umum, asosiasi biasanya juga disertai dengan *multiplicity*.
Generalisasi 	Merupakan relasi antar kelas dengan makna generalisasi-spesialisasi (umum-khusus).
Kebergantungan/*dependency* 	Merupakakan relasi antar kelas dengan makna kebergantungan antar kelas

BAB I
PENDAHULUAN

1.1. Latar Belakang

Keamanan informasi merupakan tindakan untuk melindungi informasi terhadap berbagai ancaman demi menjamin kelangsungan proses bisnis yang ada, serta mengurangi atau menghilangkan risiko dan memaksimalkan laba dan peluang bisnis untuk suatu organisasi. Keamanan informasi dapat dibentuk dengan cara menerapkan suatu set kontrol yang termasuk di dalamnya prosedur, proses bisnis, kebijakan organisasi, struktur oganisasi serta manfaat dari *software* dan *hardware*. Kontrol tersebut perlu ditetapkan, dilaksanakan, dipantau, dikaji ulang dan disempurnakan demi menjamin keamanan dan tercapainya tujuan bisnis organisasi (National Institute of Standards and Technology Gaithersburg, 2012). *United Stated National Information System Security* mendefinisikan keamanan sistem informasi sebagai perlindungan sistem informasi terhadap akses yang tidak sah atau modifikasi informasi, baik yang terjadi saat penyimpanan, pemprosesan atau transit, penolakan layanan terhadap pengguna resmi atau pemberian layanan kepada pengguna yang tidak sah, juga termasuk tindakan-tindakan yang diperlukan untuk mendeteksi dan melawan ancaman tersebut (Stoneburner, Gougen and Feringa, 2002).

Risiko/ancaman adalah sesuatu kejadian atau tindakan yang menyebabkan kerusakan atau kerugian. Sesuatu hal yang mengacu pada kondisi seseorang melakukan sesuatu yang merugikan atau kejadian (bencana) alam yang membuat hasil yang merugikan, yang memberikan dampak *negative* yang sangat banyak(National Institute of Standards and Technology Gaithersburg, 2012). Risiko dapat memberikan dampak yang cukup signifikan bagi organiasasi. Sebagai upaya mengatasi risiko maka diperlukan manajemen risiko, manajemen risiko merupakan tahapan-tahapan untuk menganalisis atau mendeskripsikan risiko, kemudian disusun beberapa strategi yang bisa diterapkan untuk meminimalisir risiko dan akibatnya (Stulz, 2008).

Menurut (National Institute of Standards and Technology Gaithersburg, 2012) penilaian risiko adalah segala proses pengelolaan risiko yang mencakup identifikasi, evaluasi, mitigasi dan pengendalian risiko terutama yang berhubungan dengan menyangkut keamanan informasi yang dapat mengancam kelangsungan usaha, strategi visi misi dan aktivitas organisasi untuk masa sekarang beserta masa yang akan datang. Menurut (Alberts and Dorofee, 2002) penilaian risiko adalah beberapa tahapan untuk menganalisia risiko, risiko tersebut dinilai, diidentifikasi, dan selanjutnya dibuatlah strategi-strategi yang bisa digunakan untuk menghambat risiko tersebut. Tahapan pelaksanaan penilaian risiko, melimiliki tahapan yang disebut tahapan penanganan yang merupakan tahapan untuk memutuskan apa yang harus dilakukan untuk mengurangi risiko, dari proses itu terdapat empat pilihan penanganan terhadap potensi risiko tersebut, yaitu *take* (terima), *treat* (kurangi), *terminate* (hindari), *transfer*. Menurut (Stoneburner, Gougen and Feringa, 2002) penilaian risiko adalah sebuah proses yang berkelanjutan dalam memitigasi, mengevaluasi, dan menilai risiko.

Penilaian risiko Keamanan Informasi (KI) menggunakan metode NIST SP 800-30 telah diteliti sebelumnya oleh (Syafitri, 2016) yang meneliti tentang Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus : Sistem Informasi Akademik Universitas XYZ), berdasarkan hasil penilaian risiko berbasis keamanan informasi, universitas yang diteliti memiliki 1 risiko tingkat tinggi, risiko tingkat sedang sebanyak 5 risiko dan 52 risiko tingkat rendah. Telah diteliti juga oleh (Nurochman, 2014) yang meneliti tentang Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan UGM Yogyakarta, berdasarkan dari hasil penelitian yang telah dilaksanakan didapatlah deskripsi profil risiko yang dapat membahayakan sistem informasi perpustakaan. Jenis risiko yang ditemukan ialah meliputi jenis risiko teknis dan risiko manusia. Risiko teknis terdiri dari listrik dengan risiko tingkat tinggi, server hang dengan deskripsi risiko level tinggi, keamanan sandi memiliki deskripsi risiko tingkat tinggi, keamanan sistem memiliki derkripsi risiko tingkat tinggi, dan otorisasi hak akses memiliki risiko tingkat sedang. Sedangkan jenis risiko yang disebabkan oleh manusia memiliki deskripsi risiko tingkat sedang.

NIST (*National Institute of Standard and Technology*) mengeluarkan rekomendasi melalui publikasi khusus 800 – 30, NIST SP 800-30 adala metode yang memberikan panduan manajemen dan penilaian risiko untuk sistem teknologi informasi yang merupakan standar dari pemerintahan *United States*. Sesuai dengan tujuan utamanya metode ini dirancang sebagai metode yang memiliki perhitungan secara matematis. Setelah membaca dan mempelajari jurnal-jurnal yang telah meneliti tentang penilaian risiko dengan menggunakan metode NIST 800-30, terdapat beberapa kelemahan atau celah yang dimiliki oleh peneliti sebelumnya, diantaranya adalah hasil *assessment* menggunakan *tools* NIST SP 800-30 berdasarkan *system characterization* yang diteliti oleh (Syafitri, 2016), yaitu hanya sebatas akses secara logika tidak secara fisikal. Hal ini dikarenakan server dari SI Akademik berada pihak ketiga. Pada penelitian (Susilo, 2017) Perlu dilakukan lagi penelitian sejenis khususnya yang dimana pengukuran menggunakan Risk Level Matrix 5x5 dan melibatkan lebih banyak perguruan tinggi sebagai obyek penelitian.

Pada penelitian ini penulis akan menjadikan 3 Sistem Akademik UIN Suska Riau yaitu *Integrated Academic Information System* (Iraise), Sistem Regristasi (Sireg) dan Penerimaan Mahasiswa Baru (PMB) sebagai studi kasus dari penelitian yang akan dilakukan. Berdasarkan wawancara yang dilakukan dengan staf divisi aplikasi Pusat Teknologi Informasi dan Pengumpulan Data (PTIPD), sistem akademik tersebut belum memiliki standar sehingga sistem ini rentan terhadap risiko, dan pada setiap pembuatan aplikasi tidak ada *cord review* serta aplikasi untuk *penetration test*-nya. Permasalahan yang kerap terjadi pada ketiga sistem informasi ini adalah *human error*, seperti kesalahan *programmer* dalam membuat *role* sehingga ada celah untuk mahasiswa bisa mengakseses *role* level dosen. Permasalahan selanjutnya yang sering terjadi adalah pada tahun ajaran baru server dari sistem ini selalu mengalami kekurangan *resource*, sehingga menyebabkan keresahan daripada pengguna sistem terkhusus mahasiswa yang ingin melakukan pengisian Kartu Rencana Studi (KRS). Pada tanggal 27 desember 2018 terjadi kebakaran *Uninterruptible Power Supply* (UPS) pada ruangan server, sehingga menyebabkan server tidak dapat digunakan sampai ada

pengadaan untuk penggantian UPS. Berdasarkan permasalahan yang terjadi, peneliti akan melakukan perancangan sebuah sistem penilaian risiko keamanan informasi menggunakan metode NIST SP 800-30 untuk memberikan level dan level risiko dari setiap *asset* yang berhubungan langsung dengan sistem akademik pada Universitas Islam Negeri Sultan Syarif Kasim Riau.

1.2. Rumusan Masalah

Rumusan permasalahan dari penelitian ini adalah bagaimana membangun Sistem Penilaian Risiko menggunakan Metode NIST SP 800-30 ?

1.3. Batasan Masalah

Pembuatan Sistem Informasi ini dilaksanakan di sistem akademik UIN Suska Riau, mengingat cakupan yang luas pada sistem akademik ini maka pada penilitian ini hanya akan melingkupi:

1. Sistem akademik yaitu Iraise, PMB, dan Sireg.
2. Hanya mealakukan penilaian risiko dalam bentuk level risiko pada *asset* yang berhubungan langsung dengan Sistem Akademik di UIN Suska Riau.
3. Memberikan rekomendasi dari kemungkinan ancaman pada *asset* yang berhubungan lamgsung dengan Sistem Akademik di UIN Suska Riau.

1.4. Tujuan

Tujuan dari perancangan sistem ini adalah untuk diterapkan metode NIST SP 800-30 dalam sistem penilaian risiko keamanan informasi dengan studi kasus pada sistem akademik UIN Suska Riau.

1.5. Sistematika Penulisan

Berikut merupakan sistematika penulisan laporan tugas akhir yang terdiri dari pendahuluan, landasan teori, metodologi penelitian, analisa dan perancangan, implementasi dan pengujian, dan yang terakhir penutup. Untuk lebih jelas lagi akan di jelaskan dibawah ini:

BAB I. PENDAHULUAN

Menjelaskan tentang latar belakang yang mendasari penelitian, rumusan masalah, tujuan penelitian, batasan masalah, tujuan dan sistematika penulisan.

BAB II. LANDASAN TEORI

Pada bab ini peneliti akan menjelaskan tentang teori singkat yang berhubungan dengan judul penelitian yaitu; penjelasan tentang sistem informasi, keamanan informasi, penilaian risiko, model pengembangan aplikasi yaitu NIST SP 800-30, sistem rekomendasi dan penelitian terkait.

BAB III. METODOLOGI PENELITIAN

Pada bab ini menjelaskan mengenai beberapa rangkaian tahapan dalam pembuatan aplikasi, mulai dari tahapan penelitian, tahap perencanaan, menentukan data, melakukan analisa menggunakan metode NIST SP 800-30, perancangan sistem, tahap implementasi dan pengujian yang digunakan, hingga kesimpulan dan saran.

BAB IV. ANALISA DAN PERANCANGAN SISTEM

Pada bab ini berisi tentang penjelasan analisa karakterisasi sistem, identifikasi ancaman pada sistem akademik, identifikasi kerentanan, analisa pengendalian sistem, penentuan kemungkinan, analisa dampak, penentuan risiko (*risk determination*) sistem akademik, rekomendasi control sistem akademik, hingga dokumentasi hasil kegiatan penilaian risiko. Melakukan analisa dan perancangan sistem penilaian risiko keamanan informasi dengan bantuan analisa seperti *usecase diagram*, *sequence diagram*,

deployment Diagram, rancangan *database*, desain menu dan antarmuka.

BAB V. IMPLEMENTASI DAN PENGUJIAN

Berisikan hasil implementasi analisa dan perancangan yang disajikan dalam bentuk lingkungan implementasi, implementasi sistem yang berisikan antarmuka sistem, serta pengujian *black box* dari setiap proses Sistem Informasi Penilaian Risiko dengan menggunakan metode NIST SP 800-30, dan pengujian User Acceptance Test (UAT).

BAB VI. PENUTUP

Berisi tentang poin-poin penting pada penelitian yang dilakukan yang berupa kesimpulan dan saran.

BAB II
LANDASAN TEORI

2.1 Sistem Informasi

Sistem merupakan serangkaian komponen-komponen yang saling berinteraksi dan bekerja sama untuk mencapai suatu tujuan yang tertentu (Pinantoan, 2008). Informasi merupakan sebuah bentuk yang dihasilkan oleh pengolahan data, data yang telah diolah tesebut menjadi berarti dan bermanfaat bagi pemiliknya dan bisa dijadikan patokan dalam pengambilan keputusan yang sedang dilakukan atau yang akan dilakukan . Fungsi utama dari informasi merupakan mengurangi ketidak pastian bagi pemakai informasi atau menambah pengetahuan (Sutabri, 2012). Sistem informasi merupakan sekumpulan komponen yang saling berhubungan, mendapatkan atau mengumpulkan, menyimpan, memproses, dan memberikan informasi sebagai penunjang pengambilan keputusan bagi pemilik atau pemakainya (Hartono, 2005).

2.2 Keamanan Informasi

Istilah keamanan informasi digunakan untuk mendeskripsikan perlindungan pada *hadware*, data, *software*, informasi, dan infrastruktur agar tidak disalah gunakan oleh pihak yang tidak berwenang (Grover, 2007). Menurut (McLeod and Schell, 2006) keamanan informasi memiliki tujuan untuk menjaga tiga kepentingan utama yaitu kerahasisaan, ketersediaan, integritas. Informasi pada sistem informasi merupakan salah suatu hal yang teramat penting untuk sebuah organisai, karena informasi adalah suatu sumber daya yang digunakan dalam strategis untuk meningkatkan nilai suatu perusahaan atau instansi. Dengan begitu informasi seharusnya dilindungi agar aman dan terbebas dari ancaman atau bahaya. Keamanan sistem informasi bertujuan agar menjauhkan suber ancaman dari sebuah sistem informasi dan juga agar membetulkan dan mendeteksi setiap kerusakan sistem yang

disebabkan oleh sumber ancaman. Keamanan informasi memiliki beberapa aspek yang harus dipahami dan dilindungi (Permatasari *et al.*, 2016). Terdapat beberapa tindakan untuk melindungi informasi atau data pada suatu sistem informasi, adapun tindakan yang dapat dilakukan ialah *presentif* (penecegahan) dan *recovery* (pengobatan) (Paryati, 2008).

2.2.1 Penilaian Risiko

Menurut(National Institute of Standards and Technology Gaithersburg, 2012), masalah keamanan sistem informasi ada 2 yaitu: "*threat*" (ancaman/risiko) dan "*vulnerability*" (kelemahan). Menurut (*National Institute of Standards and Technology* Gaithersburg, 2012) risiko atau ancaman merupakan sesuatu yang tidak pasti pada masa yang akan datang yang berkaitan dengan kerugian yang harus dipikul oleh organisasi. Berikut adalah 3 aspek yang memungkinkan terjadinya suatu ancaman atau risiko, yaitu:

1. Kemungkinan dari suatu kejadian ataupun peristiwa
2. Dampak atau kosekuensi dari risiko ketika risiko tersebut terjadi (belum terjadi)
3. Probabilitas risiko yang merupakan kemungkinan akan terjadinya suatu kejadian yang berisiko.

Bentuk ancaman-ancaman yang masuk dalam pertimbangan penilaian risiko, meliputi : *Accidental Disclosure*, kondisi alam, penambahan perangkat lunak, penggunaan *bandwith*, interferensi listrik, *intentional alteration of data*, kesalahan konfigurasi sistem, dan kegagalan operasi jaringan (National Institute of Standards and Technology Gaithersburg, 2012). Pada sebuah instansi pendidikan, ancaman atau risiko bisa datang dari bagian eksternal ataupun bagian internal. ancaman yang timbul akibat dari bagian eksternal adalah adanya peraturan perundang- undangan baru, perkembangan teknologi, bencana alam dan lainnya (Stoneburner, Gougen and Feringa, 2002). Sedangkan risiko yang muncul akibat dari bagian internal berupa dana operasional yang terbatas, sumber daya manusia yang tidak berkompeten, peralatan yang kurang atau memadai, ketidak

jelasan kebijakan prosedur, tidak kondusifnya suasana kerja, sabotase dari pegawai, dan lainnya.

2.3 NIST (National Institute of Standard and Technology) Special Publication 800-30

Dalam penilaian risiko kita perlu menetukan tujuan terlebih dahulu, tujuan bisa berasal dari proses bisnis yang ada pada suatu organisasi (Albana and Saputra, 2012). Dalam melakukan proses penilaian risiko keamanan informasi penulis membutuhkan metode yang dapat dijadikan pedoman. Berikut adalah beberapa metode yang tersedia dalam melakukan penilaian risiko keamanan informasi, contohnya adalah NIST SP 800-30, OCTAVE-S, dan COBIT metode ini biasanya digunakan untuk penilaian risiko. NIST (*National Institute of Standard and Technology*) mengeluarkan rekomendasi melalui publikasi khusus 800 – 30, panduan manajemen dan penilaian risiko untuk sistem teknologi informasi yang merupakan standar dari pemerintahan *United States*. Sesuai dengan tujuan utamanya metode ini dirancang sebagai metode yang memiliki perhitungan secara matematis. (gary stonebumer, alice goguen, 2002) dalam melakukan penilaian risiko bagi tata kelola teknologi informasi, format standar sudah ada, namun akan disesuaikan dengan proses bisnis yang ada di organisai yang bersangkutan. Secara garis besar tahapan yang dalam metodologi *Risk Assesment* meliputi:

1. Karakterisasi Sistem (*System Characterization*)

   Langkah pertama dalam penilaian risiko adalah untuk membuat karakteristik sistem, dengan cara menentukan ruang lingkup atau scope dari suatu kasus.

2. Identifikasi Ancaman (*Threat Identification*)

   Tahap ke dua berupa identifikasi ancaman, potensi ancaman bisa berasal dari luar atau dari dalam organisasi jadi harus diidentifikasi dan kemudian didokumentasikan. Sumber ancaman bisa berupa tindakan atau kejadian, intinya semua yang bisa memberikan atau menyebabkan kerusakan pada sistem informasi (National Institute of Standards and Technology Gaithersburg, 2012).

Sumber ancaman yang memungkinkan mengganggu aktivitas layanan sistem akademik antara lain:

a. Ancaman Alam

   Ancaman alam dapat dikategorikan sebagai bencana yang dapat ditimbulkan dari ancaman air seperti banjir, tsunami, intrusi air laut, kelembaban tinggi, badai, pencairan salju. Ancaman tanah: longsor, gempa bumi, gunung meletus. Ancaman alam lain: kebakaran hutan, petir, tornado,angin ribut.

b. Ancaman lingkungan / teknis

   Ancaman lingkungan meliputi: gangguanlistrik seperti putusnya aliran listrik, penurunan teganganlistrik atau kenaikan tegangan listrik secaratiba-tiba dalam jangka waktu yang lama. Medan elektromagnetik, gangguan pengerat (tikus), efek bahan kimia obat pembunuh serangga, kebocoran AC (*air conditioning*).

c. Ancaman manusia

   Ancaman yang berasal dari manusia terbagi menjadi dua ancaman dari intern organisasi Sistem Akademi dan ekstern organisasi Sistem Akademik.

3. Identifikasi Kerentanan (*Vulnerability Identification*)

   Langkah selanjutnya adalah identifikasi kerentanan, kerentanan TI secara teknis maupun non-teknis yang disebabkan atau dipicu oleh sumber-sumber ancaman. Untuk mengidentifikasi ancaman, terlebih dahulu perlu dilakukan penentuan aset yang bersangkutan dengan sistem informasi.

4. Analisa Pengendalian (*Control Analysis*)

   Langkah selanjutnya ialah analisa pengendalian, tahap ini dilakukan dengan cara mendokumentasikan dan menilai efektivitas pengendalian teknis dan non-teknis yang telah atau akan dilaksanakan oleh suatu organisasi agar meminimalkan/mengurangi suatu sumber ancaman untuk sebuah sistem informasi.

5. Penentuan Kemungkinan (*Likelihood*)

Tujuan dari langkah ini adalah untuk menentukan nilai keseluruhan kemungkinan yang menunjukkan kemungkinan bahwa kerentanan dapat dimanfaatkan oleh sumber ancaman yang diberikan kontrol keamanan yang ada atau yang direncanakan (National Institute of Standards and Technology Gaithersburg, 2012). Merujuk ke standar NIST SP 800-30 tabel 2.1 berikut ini adalah kemungkinannya :

Tabel 2. 1 Definisi kemungkinan/ kecendrungan

Tingkatan	Sebutan	Defenisi
0 -0,2	**Sangat jarang**	Hampir tidak pernah terjadi
0,2-0,4	**Jarang**	Kemungkinan terjadi tapi kecil
0,4-0,6	**Mungkin**	Mungkin saja terjadi tapi jarang-jarang
0,6-0,8	**Sering**	Kemungkinan besar terjadi
0,8-1,0	**Sangat sering**	Hampir selalu terjadi

6. Analisa Dampak (*Impact Analysis*)

Tujuan dari langkah ini adalah untuk menentukan tingkat dampak negatif yang akan dihasilkan dari ancaman berhasil mengeksploitasi kerentanan. Faktor data dan sistem untuk mempertimbangkan harus mencakup pentingnya misi organisasi, kepekaan dan kekritisan (nilai atau kepentingan), biaya yang terkait, hilangnya kerahasiaan, integritas, dan ketersediaan sistem dan data.

Tabel 2. 2 Definisi Besarnya Dampak

Tingkatan	Sebutan	Defenisi
1	Sangat kecil	Dampak kecil yang dapat diabaikan
2	Kecil	Kerusakan kecil yang mudah diperbaiki kembali
3	Sedang	Memengaruhi pencapaian beberapa sasaran

Tingkatan	Sebutan	Defenisi
4	Besar	Sasaran-sasaran penting tidak dapat tercapai
5	Sangat besar	Semua sasaran tidak dapat tercapai

7. Penentuan Risiko (*Risk Determination*)

Dengan mengalikan peringkat dari penentuan kemungkinan dan analisis dampak, tingkat risiko yang sudah ditentukan terlebih dahulu (National Institute of Standards and Technology Gaithersburg, 2012).

Rumus : Penilaian Risko = Dampak x Peluang

Tabel 2. 3 Penentuan Risiko

Kemungkinan /Dampak	**Sangat kecil**	**Kecil**	**Sedang**	**Besar**	**Sangat besar**
Sangat sering	Sedang	Tinggi	Tinggi	Ekstrim	Ekstrim
Sering	Sedang	Sedang	Tinggi	Tinggi	Ekstrim
Mungkin	Rendah	Sedang	Sedang	Tinggi	Ekstrim
Jarang	Rendah	Sedang	Sedang	Tinggi	Tinggi
Sangat jarang	Rendah	Rendah	Sedang	Sedang	Tinggi

8. Rekomendasi kontrol

Tujuan dari langkah ini adalah untuk mengidentifikasi kontrol yang dapat menghilangkan atau mengurangi risiko yang teridentifikasi, sesuai dengan operasi organisasi. Kontrol ini adalah untuk mengurangi tingkat risiko terhadap sistem dan data ke tingkat yang dapat diterima. Faktor-faktor yang perlu dipertimbangkan ketika mengembangkan kontrol mungkin termasuk efektivitas atas pilihan yang direkomendasikan (yaitu, kompatibilitas sistem), undang-undang dan peraturan, kebijakan organisasi, dampak operasional, dan keselamatan dan keandalan. Rekomendasi kontrol memberikan masukan untuk proses mitigasi risiko, di mana kontrol direkomendasikan keamanan prosedural dan teknis dievaluasi, diprioritaskan, dan diimplementasikan.

9. Dokumentasi Hasil Kegiatan

   Penulis melakukan dokumentasi dari hasil kegiatan dari penilaian risiko yang kemudian didokumentasikan dalam bentuk laporan resmi yang kemudian diberikan kepada pihak yang bersangkutan agar mereka bisa mengambil langkah untuk menerapkan beberapa rekomendasi yang telah dibuat untuk mengurangi risiko.

2.4 Sistem Rekomendasi

Sistem rekomendasi adalah suatu alat dan teknik yang menyediakan saran yang dapat dimanfaatkan oleh pengguna terkait suatu hal. Akurasi dari rekomendasi yang dihasilkan oleh sebuah sistem rekomendasi sangat bergantung pada algoritma yang digunakan. Namun, hal yang menentukan seberapa efektif suatu sistem rekomendasi tergantung pada faktor-faktor yang meliputi kualitas algoritma. Efektifitas dalam memperkenalkan pengguna terhadap item-item yang ada pada sistem rekomendasi dapat dilihat pada ketertarikan pengguna dan perasaan yakin dari pengguna dalam mencoba item-item tersebut. Hal ini menunjukkan keberhasilan dari sistem rekomendasi bergantung kepada perspektif dari pengguna (Ricci, Rokach and Shapira, 2011).

Ciri-ciri dari sistem rekomendasi yang efektif menurut (Swearingen and Sinha, 2001) adalah sebagai berikut:

1. Munculnya rasa percaya pengguna terhadap sistem.
2. Memiliki logika sistem yang transparan.
3. Memberikan rekomendasi dari item yang baru dan belum pernah dialami atau ditemui kepada pengguna.
4. Menyediakan rincian dari item-item yang direkomendasikan, termasuk gambar dan penilaian komunitas.
5. Menyediakan cara bagi pengguna untuk memperbaiki atau memperbaharui *output* rekomendasi dengan menyertakan atau tidak menyertakan jenis item tertentu.

Setelah melakukan penelitian dan mengetahui *level* risiko dari aset-aset IT yang terdapat pada organisasi, langkah selanjutnya adalah menentukan bagaimana kriteria penerimaan risiko dari aset tersebut. Kriteria ini digunakan sebagai acuan

pemberian tidakan yang akan dilakukan terhadap aset-aset yang memiliki nilai risiko kritis dan memiliki dampak yang ditimbulkan jika terjadi kegagalan keamanan informasi pada organisasi. Tujuan dari identifikasi dan evaluasi penanganan risiko ini adalah untuk menentukan pilihan penanganan risiko jika risiko yang timbul tidak langsung diterima akan tetapi perlu dilakukan pengelolaan lebih lanjut dengan menggunakan kriteria-kriteria penerimaan risiko yang telah ditentukan. Berikut ini adalah kriteria-kriteria dalam penerimaan risiko berdasarkan standar ISO/IEC 27002:2013 yang dapat dikategorikan sebagai berikut:

1. Risiko diterima (*Risk Acceptance*)
   Menerima risiko dengan menerapkan kontrol keamanan yang sesuai.
2. Risiko direduksi (*Risk Reduction*)
   Menerima risiko yang terjadi dengan melakukan tindakan pencegahan risiko tersebut menggunakan kontrol keamanan untuk mengurangi dampak yang ada sampai pada *level* yang dapat diterima oleh organisasi.
3. Risiko ditolak (*Risk Avoidance*)
   Risiko ditolak dengan cara menghilangkan atau menonaktifkan aset hingga mendapatkan solusi terbaik yang dapat mengurangi risiko. Biasanya pada penanganan risiko ini akan memberikan biaya terhadap proses bisnis organisasi, sehingga keputusan yang diambil untuk penanganan risiko tersebut adalah dengan menghindari risiko tersebut.
4. Risiko dialihkan (*Risk Transfer*)
   Menerima risiko dengan cara mentransfer risiko kepada pihak ketiga (Asuransi, *vendor, supplier,* atau pihak tertentu) untuk penanganan dan mengurangi dampak yang ditimbulkan.

Berikut adalah tabel matriks kriteria penerimaan risiko yang dapat dijadikan sebagai panduan oleh organisasi yang dapat dilihat pada tabel 2.4 berikut ini.

Tabel 2.4 Matriks Kriteria Penerimaan Risiko

Probalitas Ancaman (PA)	**Biaya Pemulihan (BP)**		
	LOW	**MEDIUM**	**HIGH**
HIGH	Risk Acceptance	Risk Avoidance	Risk Transfer
MEDIUM	Risk Acceptance	Risk Reduction	Risk Transfer
LOW	Risk Acceptance	Risk Reduction	Risk Transfer
	HIGH	**MEDIUM**	**LOW**
	Biaya Transfer Resiko (BR)		

Tabel matriks kriteria penerimaan risiko merupakan hubungan antara variabel berikut : probabilitas ancaman (*threat probability*), biaya pemulihan (*recovery cost*) akibat atau dampak dari penerimaan risiko, dan biaya transfer risiko (*risk transfer cost*) kepada pihak ketiga. Tabel 2.14 di atas menggunakan prinsip logika AND, untuk penjelasannya sebagai berikut:

1. Jika salah satu variabel berlogika **LOW** maka resiko diterima dan sebaliknya jika salah satu nilai variabel berlogika **HIGH** maka resiko ditolak.
2. Kriteria resiko diterima dapat dikembangkan dengan kriteria tambahan sebagai berikut:
   a) Jika biaya pemulihan **lebih kecil** daripada biaya transfer resiko, maka resiko diterima dengan status *Risk Acceptance;*
   b) Jika biaya pemulihan **lebih besar** daripada biaya transfer resiko, maka resiko diterima dengan status *Risk Transfer;*
   c) Jika biaya pemulihan **sama dengan** biaya transfer resiko, maka resiko diterima dengan status *Risk Reduction*, yaitu direduksi dengan menggunakan pengendalian kontrol keamanan sampai pada level diterima oleh organisasi, kecuali jika probabilitas ancaman bernilai **HIGH** maka resiko ditolak (*Risk Avoidance*).

Untuk penjelasan tambahan dari kriteria penerimaan risiko dapat dilihat pada tabel kebenaran kriteria penerimaan risiko di bawah ini.

Tabel 2.5 Kebenaran Kriteria Penerimaan Risiko

No	PA	BP	BR	Kriteria
1	LOW	LOW	HIGH	*Risk Acceptance*
2	MED	LOW	HIGH	*Risk Acceptance*
3	HIGH	LOW	HIGH	*Risk Acceptance*
4	LOW	MED	MED	*Risk Reduction*
5	MED	MED	MED	*Risk Reduction*
6	HIGH	MED	MED	*Risk Avoidance*
7	LOW	HIGH	LOW	*Risk Transfer*
8	MED	HIGH	LOW	*Risk Transfer*
9	HIGH	HIGH	LOW	*Risk Transfer*

2.5 Penelitian Terkait

Beberapa penelitian terdahulu yang pernah dilakukan untuk penilaian risiko IT menggunakan NIST SP 800-30 antara lain :

Tabel 2. 6 Tabel Penelitian Terkait

No	Penulis	Judul	Tahun	Metode	Hasil
1	Wenni Syafitri	Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)	2016	NIST 800-30	Berdasarkan hasil penilaian risiko pada penelitian ini menghasilkan deskripsi tingkatan ancaman yang dimiliki universitas xyz: 1 ancaman tingkat tinggi, 5 ancaman tingkat sedang, dan 52 ancaman tingkat rendah.
2	Susilo	Analisa Tingkat Risiko Tata Kelola Teknologi Informasi Perguruan Tinggi Menggunakan Model Framework National Institute of Standards & Technology (NIST) Special Publication 800-30 dan IT General Control Questionnaire (ITGCQ)	2017	NIST *Special Publication* 800-30 dan *Information Technology General Control Questionnaire* (ITGCQ)	Hasil Pengukuran Risiko menggambarkan bahwa, tingkat risiko tata kelola teknologi informasi PTS XYZ berada pada level *High Risk;*

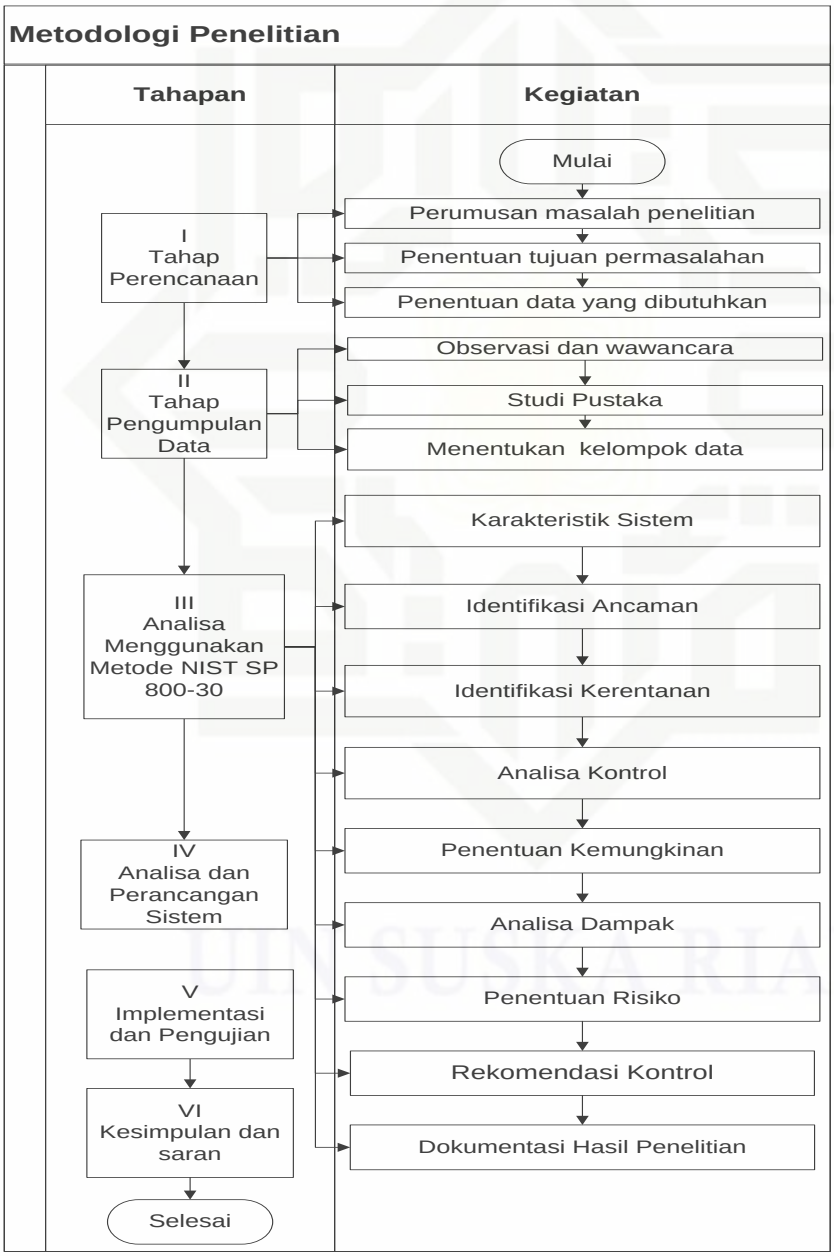
No	Penulis	Judul	Tahun	Metode	Hasil
3	Ucu Nugraha	Manajemen Risiko Sistem Informasi Pada Perguruan Tinggi Menggunakan Kerangka Kerja Nist Sp 800-300	2016	NIST SP 800-30	Hasil dari penelitian manajemen risiko ini berupa beberapa sumber ancaman yang berpotensi untuk menimbulkan sebuah risiko pada teknologi informasi ini, diantaranya keamanan sistem informasi yang berisiko tinggi, tingginya tingkat risiko akan hangnya backup dari server sistem informasi, dan risiko tingkat sedang pada keaman password.
4	Arif Nurochman	Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan UGM Yogyakarta	2014	NIST SP 800-30	*Framework* NIST SP (*National Institute of Standards & Technology Special Publication)*800- 30 memiliki metode pengawasan secara menyeluruh melalui evaluasi pelaksanaan manajemen risiko sistem informasi perpustakaan dalam siklus hidup pengembangan sistem informasi.
5	Fathoni Mahardika	Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)	2017	NIST SP 800-30	STMIK Sumedang memiliki level risiko keamanan informasi yang *Moderate*, dimana untuk risiko *adversarial* terdiri dari: 20 tingkat *High*, 46 tingkat *Moderate*, 10 tingkat *Low*, 2 tingkat *Very Low*. Sedangkan untuk risiko *non-adversarial* terdiri dari : 2 tingkat *Very High*, 5 tingkat *High*, 9 tingkat *Moderate*, 1 *Low*.

No	Penulis	Judul	Tahun	Metode	Hasil
6	Mohamed Ghazouani, sophia Faris Ensem, Hicham Medromi Ensem, dan Adil Sayouti	Keamanan Informasi Penilaian Risiko - Sebuah Pendekatan Praktis dengan Matematika Penyusunan Risiko	2014	NIST SP 800-30	Secara umum, keamanan SI memiliki beberapa tujuan. Keselamatan, kemudian, harus melindungi informasi-informasi perusahaan agar tidak mengalami kerusakan atau kehilangan data yang merupakan asset perusahaan. Dalam hal ini tujuan tersebut bisa di penuhi, dan penelitian ini merekomendasikan beberapa tindakan untuk melindungi asset perusahaan tersebut.
7	Meri Andani	Manajemen Risiko Keamanan Aplikasi Sistem Informasi Laporan Harian PKS & PPKO Online Pada PTPN V Menggunakan Metode NIST SP 800-30	2014	NIST SP 800-300	Hasil dari penilaian risiko yang terjadi pada sistem laporan harian produksi ini memberikan rekomendasi control yang disarankan terhadap ancaman risiko *human error* yaitu membuat pembatasan hak akses sesuai dengan tingkat kepentingan dan melakukan pengawasan secara internal terhadap apa saja yang dikerjakan.

BAB III
METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Ada banyak tahapan-tahapan yang dilakukan dalam penyusunan Tugas Akhir, berikut merupakan tahapan-tahapan untuk menyusun atau membuat Tugas Akhir :



Gambar 3. 1 *Flowchart* Metodologi Penelitian

Tabel 3.1 adalah langkah-langkah dalam penyusunan atau pembuatan penelitian ini, berikut ini adalah penjelasan lebih lengkap untuk Gambar 3.1:

3.2 Tahap Perencanaan

Dalam tahap perencanaan yang merupakan tahap awal penelitian, kegiatan yang dilakukan adalah sebagai berikut:

A. Perumusan Masalah Penelitian

Menentukan tentang masalah apa saja yang akan dibahas dalam penelitian penilaian risiko yang dilakukan pada sistem akademik Uin Suska Riau.

B. Menentukan Tujuan Penelitian

Penelitian Untuk mendukung pencapaian sasaran penelitian, tahapan selanjutnya adalah penentuan tujuan dari yang dilakukan. Tujuan dilakukannya penelitian adalah sebagai berikut:

1. Membuat Sistem Informasi Penilaian Risiko Menggunakan Metode NIST SP 800-30 terhadap sistem akademik (Iraise, PMB, dan Sireg) di UIN SUSKA RIAU.
2. Menentukan hasil penilaian risiko keamanan teknologi informasi dan memberikan rekomendasi terhadap perusahaan.

C. Menentukan Data

Pada tahap ini penulis akan melakukan studi pustaka untuk mempermudah penulis dalam melakukan analisis, maka perlu ditentukan beberapa data seperti:

1. Teori-teori yang berhubungan dengan manajemen risiko TI, dan keamanan TI.
2. Teori metode NIST SP 800-30.
3. Menentukan kebutuhan data primer dan data sekunder.

3.3 Tahap Pengumpulan Data

Tahap ini merupakan tahap yang dilakukan setelah tahap perencanaan. Setelah data ditentukan, maka selanjutnya adalah mengumpulakan data tersebut. Tahapan ini berisi tentang proses dalam pengumpulan data, berupa data primer dan skunder. Tahapannnya adalah sebagai berikut:

A. Pengumpulan Data

Pada penelitian ini penulis akan melakukan dua teknik yang digunakan dalam pengumpulan data yaitu observasi dan wawancara, observasi dan wawancara ini dilakukan di Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) yang dilakukan untuk mendapatkan informasi tentang sistem akademik UIN Suska Riau, yaitu IRaise, Sireg, dan PMB.

B. Studi Pustaka

Pada tahap ini penulis melakukan pencarian referensi untuk teori-teori yang sesui dengan topik penelitian yang di lakukan, pada penelitian ini penulis mendapatkan sumber referensi dari buku, publikasi hasil penelitian, artikel dan situs internet serta sumber informasi lainnya yang berkaitan dengan penelitian ini.

C. Menentukan Data Primer dan Data Sekunder

Berikut ini adalah penjelasan tentang data primer dan skunder serta data skunder dan primer yang diperlukan oleh penulis:

1. Data Primer ini adalah data yang langsung didapat dari tempat penelitian, dalam tugas akhir ini data primernya adalah data yang langsung diperoleh dari pihak Iraise, PMB, dan Sireg di UIN Suska Riau.
2. Data skunder adalah data yang sudah ada atau tersedia, pada tugas akhir ini data sekunder yang diperoleh penulis ialah data dari buku-buku, jurnal dan internet sebagai bahan referensi.

3.4 Analisa Menggunakan Metode NIST SP 800-30

Kegiatan yang akan penulis lakukan pada tahapan penilaian risiko yang dilakukan dengan menggunakan metode NIST SP 800-30 untuk mendukung penelitian penilaian risiko di sistem akademik UIN Suska Riau adalah sebagai berikut:

1. Karakterisasi Sistem (*System Characterization*)

   Karakterisasi sistem adalah langkah pertama yang dilakukan untuk penilaian risiko, membuat karakterisasi sistem yaitu dengan cara

menentukan ruang lingkup sistem informasi. Pada tahapan karekterisasi sistem ini, penulis akan mengidentifikasikan proses bisnis dari sistem akademik yang merupakan Iraise, PMB, dan Sireg di UIN Suska Riau dengan menggunakan teknik pengumpulan informasi yang berupa wawancara dan observasi.

2. Identifikasi Ancaman (*Threat Identification*)

   Pada tahapan identifikasi ancaman ini penulis akan melakukan wawancara dan observasi di sistem akademik yang ada di UIN Suska Riau, hal ini dilakukan dengan tujuan untuk mengidentifikasi ancaman. Kemudian selanjutnya melakukan dokumentasi dari hasil wawancara dan observasi yang telah dilakukan. Dapat dilihat pada tabel 3.1 berikut ini:

Tabel 3. 1 Identifikasi ancaman pada Sistem Akademik UIN Suska Riau

Aset	Kerentanan	Ancaman	*Potential Cause*
Hardware: Komputer Server UPS	Kurangnya skema pergantian perangkat keras secara berkala	Perusakan peralatan atau media	*Maintenance* yang tidak teratur
	Kerentanan terhadap kelembapan, debu, kotoran.	Debu, korosi, pendingin, air	Kerusakan fisik pada server
	Kerentanan terhadap nilai informasi yang tersimpan pada PC	Pencurian	Kurangnya pengamanan
	Kerentanan terhadap voltase yang tidak stabil	Hilangnya pasokan listrik	Korsleting listrik
	Supply listrik yang tidak Stabil	Hilangnya pasokan listrik	Pemadaman Listrik
	Beban kerja server yang tinggi	AC diruangan server mati/rusak	Server overheat
	Pertambahan memori yang cepat dalam pemrosesan data	*Server* kekuranang *resource*	Kapasitas memori server yang sudah tidak memenuhi kebutuhan

Aset	Kerentanan	Ancaman	*Potential Cause*
Data: Data nilai mahasiswa	Redudansi data	Data tidak lengkap	Kesalahan dalam penginputan dan penghapusan data
	Kurangnya salinan *back-up*	Data hilang	Organisasi tidak melakukan prosedur *back-up*
	Jaringan internet kurang optimal	Data tidak lengkap	Speed koneksi internet yang lemah dan tidak stabil
	Kesalahan penempatan hak akses	Pembobolan data	Tidak ada penggunaan hak akses
	Terlalu banyak data yang Diinputkan	Database penuh	Server down
	Kurangnya dokumentasi *user manual* untuk aplikasi	Kesalahan pengguna	Kurangnya dokumentasi (*user manual*) untuk karyawan baru
	Kurangnya mekanisme identifikasi dan otentifikasi pengguna aplikasi	Aplikasi terserang *hacker*	Password tidak pernah diganti
Layanan teknologi informasi: Iraise Sistem Regristasi Sistem Penerimaan Mahasiswa Baru	Karyawan kurang memperhatikan pentingnya antivirus	Aplikasi terserang virus	PC terserang virus
	Tidak ada atau tidak cukup pengujian perangkat lunak	Penyalahgunaan wewenang pada hak akses yang dimiliki	Staf mengetahui kelemahan pada aplikasi
	Karyawan kurang teliti dan kompeten	Aplikasi eror	Kesalahan coding pada fungsional software
	Jalur komunikasi yang tidak dilindungi	Penyadapan informasi penting melalui jaringan Celah masuknya hacker *Remote Spying*	Lemahnya keamanan di sistem internal TI
Perangkat jaringan (network)	Manajemen jaringan yang tidak cukup (ketahanan routing) Sambungan kabel yang buruk	Jaringan LAN sering terganggu	Kurangnya mekanisme pemantauan terhadap jaringan

Aset	Kerentanan	Ancaman	*Potential Cause*
	Kualitas jaringan yang kurang baik	Konektifitas internet yang susah didapatkan	Gangguan jaringan pada provider
	Bencana alam dan kerjadian yang tidak terduga	Koneksi terputus	Kerusakan pada infrastruktur jaringan
Karyawan (People)	Karyawan kurang teliti	Kesalahan penginputan dan penghapusan data	Kesalahan pengolahan data
	Pelatihan keamanan yang tidak cukup	Penyalahgunaan wewenang pada hak akses yang dimiliki Password PC diketahui orang lain	Staf tidak logout ketika meninggalkan komputer

3. Identifikasi Kerentanan (*Vulnerability Identification*)

   Pada langkah ini penulis akan mengembangkan daftar kekurangan maupun kelemahan dari sistem informasi akademik yang ada UIN SUSKA (kerentanan sistem) yang disebabkan atau dipicu oleh sumber-sumber ancaman.

4. Analisa Pengendalian (*Control Analysis*)

   Langkah selanjutnya ialah penulis akan menganalisa pengendalian kerentanan sistem, tahap ini dilakukan dengan cara mendokumentasikan dan menilai efektivitas pengendalian teknis dan non-teknis yang telah atau akan dilaksanakan oleh Universitas Islam Negeri ini untuk meminimalkan kemungkinan ancaman pada sistem informasi akademiknya.

5. Penentuan Kemungkinan (*Likelihood*)

   Pada tahap ini penulis akan mengajukan kusioner untuk penentuan nilai keseluruhan dari kemungkinan/kecendrungan pada sumber ancaman di sistem akademik UIN Suska Riau.

6. Analisa Dampak (*Impact Analysis*)

   Pada tahapan ini penulis mengajukan kusioner untuk menentukan tingkatan dari suatu dampak negative yang dihasilkan oleh sumber ancaman yang ada di sistem akademik UIN Suska Riau.

7. Penentuan Risiko (*Risk Determination*)

   Pada tahap ini penulis menetapkan peringkat risiko dari yang terendah ke tertinggi, dengan cara mengalikan nilai atau tingkat dari kemungkinan dan dampak, kemudian tingkat risikonya ditentukan melalui tabel matrik penilaian risiko.

8. Rekomendasi Kontrol

   Pada langkah ini sistem akan membuatkan rekomendasi untuk risiko yang terdeteksi, langkah ini berguna untuk mengidentifikasi kontrol yang dapat mengurangi atau menghilangkan risiko yang teridentifikasi, sesuai dengan operasi organisasi. Rekomendasi yang di buat adalah berdasarkan pada metode NIST SP 800-30.

9. Dokumentasi Hasil Kegiatan

   Pada tahap ini penulis melakukan dokumentasi dari hasil kegiatan dari penilaian risiko yang kemudian didokumentasikan dalam bentuk laporan resmi, yang kemudian diberikan kepada pihak yang bersangkutan agar mereka bisa mengambil langkah untuk menerapkan beberapa rekomendasi yang telah dibuat untuk mengurangi risiko.

3.5 Analisis dan Perancangan Sistem

Analisa dan perancangan sistem merupakan kegiatan *multitasking* yang berfokus pada perancangan dari pembangunan sebuah program *softwere* yang bisa berupa struktur data, arsitektur sistem informasi, perancangan antarmuka, dan *coding* yang akan dibuat yang berdasarkan analisis metode sebelumnya, kemudian dilanjutkan dengan tahap perancangan sistem yang bertujuan untuk membuat rancagan tentang sistem yang akan dibangun agar pengguna mengerti saat pengoprasian sistem yang akan dibangun.

3.6 Tahapan Implementasi dan Pengujian Sistem

Pada tahap implementasi dan pengujian sistem ini, penulis akan melakukan pengujian pada setiap *unit* sistem informasi yang telah dibangun dengan tujuan agar seluruh fungsi dari bagian sistem informasi tersebut tidak bertolak belakang dengan *goal* yang telah dibuat sebelum pembangunan sistem informasi. Tahapan ini dilakukan untuk memastikan tidak ada kesalahan (*error*) dan membuat keluaran (*output*) yang ada sesuai dengan tujuan yang diinginkan.

3.7 Kesimpulan dan Saran

Pada tahap kesimpulan penulis akan memberikan kesimpulan yang berupa poin-poin penting dari hasil penelitian, yang bertujuan untuk mengetahui keberhasilan dan kesesuian sistem yang telah dirancang dan dibangun, kemudian memberikan saran tentang topik yang dibangun, sehingga dapat lebih dikembangkan lagi tentang sistem penilaian risiko keamanan informasi untuk peneliti selanjutnya.

BAB IV
ANALISA DAN PERANCANGAN SISTEM

Pada bab ini menjelasakan tentang analisis dan pembahasan tahapan-tahapan yang dilakukan dalam *assessment* atau penilaian risiko keamanan informasi menggunakan NIST SP 800-30 terhadap Sistem Akademis UIN Suska Riau. Berikut adalah Flowchart dari NIST SP 800-30:

Gambar 4. 1 Tahapan *Assesment* NIST SP 800-30

Pada tahap awal yang dilakukan adalah karakterisasi sistem atau menentukan ruang lingkup suatu sistem informasi, tujuan dari karakterisasi sistem yaitu untuk mengetahui batas-batas dari sistem akademik UIN Suska Riau. Tahap kedua yang dilakukan adalah identifikasi ancaman, indetifikasi ancaman bertujuan

untuk menentukan ancaman serta kelemahan yang mungkin terjadi dan diterima oleh sistem akademik serta mengukur risiko yang ditimbulkan terhadap kelangsungan proses bisnis Sistem Informasi Akademik.

Pada tahap ketiga yang dilakukan adalah identifikasi kerentanan, identifikasi kerentanan dilakukan untuk mengembangkan kelemahan atau kekurangan yang disebabkan oleh sumber ancaman. Tahap keempat adalah analisa pengendalian, tahap analisa pengendalian dilakukan untuk mengetahui bagai mana cara PTIPD menangani ancaman yang pernah terjadi pada sistem akademik. Tahap selanjutnya adalah penentuan kemungkinan, penentuan kemungkinan dilakukan untuk menentukan frekuensi dari sebuah sumber ancaman. Tahap yang keenam adalah analisa dampak, tahap analisa dampak dilakukan untuk menentukan kelemahan uang dihasilkan oleh sumber ancaman. Pada tahap ketuju adalah penentuan risiko, tahap penentuan risiko dilakukan untuk menentukan tingkat ancaman dari suatu sumber ancaman. Tahap kedeleapan adalah rekomendasi kontrol, tahap rekomendasi kontrol ini digunakan unruk memberikan rekomendasi berdasarkan tingkat ancaman yang ditimbulkan. Selanjutnya tahap terakhir adalah dokumentasi, tahap ini dilakukan untuk mendokumentasikan hasil kegiatan penilaian risiko.

Membuat lembar kerja *assessment* atau penilaian risiko yang berfokus pada aset Sistem Informasi Akademik dan tahapan-tahapan pada dokumen NIST SP 800-30. Hasil dari *assessment* yang dilakukan adalah tingkat risiko dariseluruh sumber ancaman yang ada saat ini pada Sistem Akademik UIN Suska Riau. Pada tahap perancangan sistem penulis akan membuat rincian kebutuhan sistem dari hasil analisis menjadi bentuk perancangan perangkat lunak yang terdiri dari *use case diagram, sequence diagram, deployment diagram, dan database diagram* agar dimengerti oleh pengguna.

4.1 Karakterisasi Sistem

Sistem Akademik UIN Suska Riau yang terdiri dari Integrated Academic Information System (Iraise), Sistem Regristasi (Sireg) dan Sistem Informasi Penerimaan Mahasiswa Baru (PMB). Sistem informasi PMB adalah sistem

informasi yang diperuntukkan untuk calon mahasiswa yang ingin mendaftarkan diri melalui jalur mandiri di salah satu bidang ilmu pada Universitas Islam Negri Sultan Syarif Kasim Riau, Sistem Regristasi atau Sireg merupakan sistem informasi yang diperuntukkan kepada calon mahasiswa baru yang ingin melengkapi persyaratan untuk menjadi mahasiswa di salah satu bidang ilmu di UIN Suska Riau, dan IRaise adalah sistem informasi akademik bagi mahasiswa dan Dosen UIN Suska Riau yang digunakan untuk mengisi Kartu Rencana Studi (KRS), dan mengisi nilai. Berdasarkan wawancara yang dilakukan dengan staf divisi aplikasi PTIPD, ketiga sistem tersebut belum memiliki standar yang membuat sistem ini rentan terhadap risiko, dan pada setiap pembuatan aplikasi tidak ada *cord review* serta aplikasi untuk *penetration test*-nya.

Berdasarkan hasil wawancara yang dilakukan dengan Kepala Aplikasi di UIN Suska Riau, Sistem Akademik UIN Suska Riau memiliki 4 jenis aset yaitu: Perangkat Keras (*Hardwar*e), Perangkat Lunak (*Software*), Informasi (*Information*), dan Sumber Daya Manusia (*People*). Aset yang tergolong pada *hardware* ialah komputer, server, dan UPS. Aset yang tergolong pada *software* adalah Sistem Regristasi (Sireg), sistem Penerimaan Mahasiswa Baru (PMB) dan Iraise. Aset yang tergolong dalam Informasi (*Information*) adalah data informasi nilai mahasiswa.

Tabel 4. 1 Karakterisasi Sistem

No	Kelompok	ID Aset	Aset	Proses Bisnis
1	Informasi (*Information*)	IN-001	Informasi Nilai Mahasiswa	Dosen login ke Iraise untuk menginput nilai mahasiswa, dosen bisa mengolah nilai mahasiswa. Mahasiswa hanya bisa mendapatkan akses *view* untuk informasi nilai mahasiswa.
2	Perangkat Keras (*Hardwar*e)	HD-001	Server	Melayani permintaan komputer *client* dan menyediakan resource untuk digunakan bersama, baik untuk perangkat keras atau aplikasi.
		HD-002	Komputer	Pegawai menggunakan komputer untuk berbagai keperluan organisasi.
		HD-003	Jaringan	Jaringan di UIN Suska memiliki topologi *Mesh*
		HD-004	UPS	*Uninterruptible Power Supply* (UPS) digunakan untuk menjadi baterai *backup*

No	Kelompok	ID Aset	Aset	Proses Bisnis
3	Informasi (*Information*)	SW-001	IRaise	IRaise digunakan untuk hampir seluruh urusan akademis di UIN Suska, penggun aplikasi ini adalah mahasiswa dan pegawai pegawai di UIN Suska.
		SW-002	Sistem Regristasi (Sireg)	Sistem Regristasi (Sireg) digunakan oleh mahasiswa baru yang sudah menyelesaikan pembayaran uang kuliah
		SW-003	Sistem informasi Pendaftaran Mahasiswa Baru (PMB)	Sistem informasi Pendaftaran Mahasiswa Baru (PMB) digunakan oleh calon mahasiswa yang melakukan pendaftaran dengan jaur mandiri.
4	Manusia (*People*).	SDM-001	Karyawan	Karyawan orang yang melakukan tugasnya dibidangnya masing-masing

4.2 Identifikasi Ancaman Sistem Akademik

Sebelum melakukan penilaian risiko, terlebih dahulu diperlukan untuk mengidentifikasi ancaman-ancaman yang dapat mengancam keamanan *asset* informasi Sistem Akademik UIN Suska Riau. Ancaman yang dimaksudkan adalah merupakan kejadian yang memiliki kemungkinan untuk terjadi kembali bahkan sering terjadi baik disebabkan oleh faktor yang berasal dari bagian eksternal maupun bagian internal perusahaan seperti bencana alam, gangguan fasilitas umum, sosial, dan operasional. kemunculannya dengan menggunakan rentang nilai sebagai berikut.

Daftar ancaman dan kelemahan dapat disimpulkan dari hasil wawancara dan diskusi dengan pegawai PTIPD pada bagian *software* dan jaringan. Berikut adalah tabel daftar ancaman pada aset Sistem Akademik UIN Suska Riau yang teridentifikasi.

Tabel 4. 2 Identifikasi Ancaman pada Aset

No.	Nama Kejadian	Keterangan	Kode
1	Akses Ilegal (*Unauthorized Access*)	Akses tidak sah dari seseorang yang tidak memiliki kepentingan.	T1
2	Serangan Virus (*Virus Attack, Ex: Malware, Ransomware, Trojan*)	Pengrusakan fungsional pada perangkat lunak akibat virus digital.	T2
3	*Hackers* (*Intruders*)	Akses tidak sah dari seseorang yang tidak memiliki kepentingan melalui jaringan komputer.	T3

No.	Nama Kejadian	Keterangan	Kode
4	Pencurian Aset (*Theft of Asset*)	Pemindahan tanpa izin dari pihak diluar instansi.	T4
5	Bencana Alam (*Nature Disaster*)	Fenomena alam yang berpotensi mengancam keberadaan aset (Gempa bumi, banjir, petir, angin kencang).	T5
6	Kebakaran (*Fire*)	Pembakaran tidak terkawal akibat konselting arus listrik, individu. yang mengancam keberadaan aset.	T6

Berikut adalah tabel kelemahan yang mungkin dimiliki oleh masing-masing aset Sistem Akademik UIN Suska Riau yang teridentifikasi.

Tabel 4.3 Identifikasi Kelemahan pada Aset Sistem Akademik Uin Suska

No.	Nama Kejadian	Keterangan	Kode
1	Kerusakan Data (*Data Corruption*)	Kerusakan terhadap data akibat tidak adanya pemeliharaan terhadap media penyimpanan data atau hal lainnya.	V1
2	Kesalahan SDM (*Human Error*)	Salah penginputan data, pengoperasian aset, kelalaian saat bertugas.	V2
3	Gangguan Perangkat Keras (*Hardware Failure*)	Tidak beroperasi aset atau perangkat keras sebagai mana mestinya.	V3
4	Gangguan Sumber Daya Listrik (*Power Failure*)	Tidak ada suplai energi listrik untuk mengoperasikan perangkat keras.	V4
5	Kesalahan Pengiriman Data (*Data Missing Recipient*)	Kesalahan pengiriman data yang mengakibatkan data tidak sampai pada tujuan.	V5
6	Kesalahan Fungsional Perangkat Lunak (*Software Bug*)	Fungsional sistem sebagaimana mestinya tidak berjalan.	V6
7	Pembaharuan Aplikasi	Tidak ada kontrol terhadap *patching* (*upate*) sistem operasi, aplikasi.	V7
8	Tidak ada kontrol pengawasan	Proses pemeliharaan (*maintanance*) dan pengawasan (*monitoring*) tidak terpantau.	V9
9	Respon pihak eksternal pada layanan	Respon yang diberikan oleh pihak eksternal terhadap layanan yang dikontrak seperti (jaringan internet) tidak tepat waktu	V10
10	Tenaga ahli kurang	Tidak ada SDM yang berkompeten pada suatu bidang dapat menghambat operasional bisnis.	V11

Setelah mendapatkan daftar ancaman dan kelemahan yang teridentifikasi pada aset Sistem Akademik UIN Suska Riau, selanjutnya menentukan daftar ancaman dan kelemahan yang relevan terhadap aset yang sudah diidentifikasi pada sub bab sebelumnya. Berikut adalah pemetaan daftar aset dan daftar gangguan keamanannya.

Tabel 4.4 Pemetaan Daftar Aset dan Gangguan Keamanan

Kode Aset	Kemungkinan Ancaman						Kemungkinan Kelemahan									
	T1	T2	T3	T4	T5	T6	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10
IN-001	■		■			■	■	■			■				■	
HD-001	■			■		■		■	■	■				■	■	■
HD-002	■			■		■		■	■	■		■	■		■	■
HD-003	■					■		■	■	■				■	■	■
HD-004	■			■		■		■	■	■				■	■	■
SW-001		■	■					■	■		■	■	■	■		
SW-002		■	■					■	■		■	■	■	■		
SW-003		■	■					■	■		■	■	■	■		
SDM-001	■		■				■	■	■		■			■		■

Setelah proses pemetaan tersebut, selanjutnya dilakukan perhitungan nilai ancaman (*threat & vulnerable*) dari setiap aset yang dapat dilihat pada lampiran. Berikut adalah hasil rekapitulasi nilai ancaman pada masing-masing aset Sistem Akademik UIN Suska Riau.

4.3 Identifikasi Kerentanan Sistem Akademik

Mengidentifikasi kerentanan pada Sistem Akademik UIN Suska Riau, penulis melakukan wawancara terhadap kepala bagian aplikasi di PTIPD, data kerentanan dibuat berdasarkan kelompok dari sebuah aset. Penjelasan lebih jelas dapat dilihat pada tabel di bawah ini, berikut adalah kerentanan pada setiap aset Sistem Akademik UIN Suska Riau :

Tabel 4. 5 Identifikasi Ancaman

Aset	Kerentanan
Information: Informasi nilai mahasiswa	Kesalahan dalam penginputan dan penghapusan data
	Organisasi tidak melakukan prosedur backup
	Salah input dan hapus data
	Pembobolan data
	Terserang virus

Aset	Kerentanan
Hardware :	
Server	Kurangpengaman organisasi
	Maintenance yang tidak teratur
	Kerusakan fisik pada server
	Korsleting listrik
	Server *overheat*
	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori penuh)
Komputer	Kurang pengaman organisasi
	Maintenance yang tidak teratur
	Kehilangan data
	Kehilangan perangkat
	Terserang virus
UPS	Korsleting listrik
	Pemadaman listrik
	Keruskan pada perangkat
Jaringan	Lemah keamanan di sistem internal TI
	Kurang mekanisme peman-tauan terhadap jaringan
	Gangguan jaringan
	Kerusakan pada infrastruktur jaringan
	Kesalahan dalam melakukan konfigurasi *access Point*
	Kabel digigit oleh hewan
Karyawan (*People*)	Kurang training prosedur penggunaan TI yang diberikan
	Kurang sosialisasi tentang regulasi dan sanksinya
	Salah input dan hapus data
	Kurang mekanisme pemantauan
Teknologi informasi: Iraise Sistem Regristasi (Sireg) Sistem Penerimaan Mahasiswa Baru (PMB)	Kurang dokumentasi
	Sistem tidak dapat di akses
	Kesalahan *coding* pada fungsional *software*
	Pembobolan data

4.4 Analisa Pengendalian Sistem Akademik

Dari observasi melalui wawancara dan kusioner yang telah dilakukan, pengendalian risiko atau ancaman yang dilakukan oleh pihak PTIPD ialah dengan cara menangani berdasarkan aset dan kelompok aset pada sistem informasi. Setiap aset memiliki potensi ancaman dan potensi ancaman ini akan diberikan penanganan atau pengendalian, untuk lebih jelas lagi berikut adalah penanganan potensi anacaman pada sistem akademik UIN Suska Riau:

Tabel 4. 6 Analisa Pengendalian

Aset	Potensi Ancaman	Penanganan
Information: Data informasi nilai mahasiswa	Kesalahan dalam penginputan dan penghapusan data	Dilakukan pengecekan
	Organisasi tidak melakukan prosedur backup	Dilakukan *Backup* secara teratur
	Salah input dan hapus data	Dilakukan pengecekan
	Pembobolan data	Tingkatkan keamanan
	Terserang virus	*Maintenance* secara teratur
Hardware :		
Server	Kurang pengaman organisasi	Tingkatkan keamanan
	Maintenance yang tidak teratur	*Maintenance* secara teratur
	Kerusakan fisik pada server	*Maintenance*
	Korsleting listrik	*Maintenance*
	Server *overheat*	*Maintenance*
	Kapasitas memori server yang sudah tidak memenuhi kebutuhan (memori penuh)	Penambahan memori
Komputer	Kurangnya pengaman organisasi	Tingkatkan keamanan
	Maintenance yang tidak teratur	*Maintenance* secara teratur
	Kehilangan data	Tingkatkan keamanan
	Kehilangan perangkat	Tingkatkan keamanan
	Terserang virus	*Maintenance* secara teratur
UPS	Korsleting listrik	*Maintenance*
	Pemadaman listrik	*Maintenance*
	Keruskan pada perangkat	*Maintenance*
Jaringan	Lemah keamanan di sistem internal TI	Tingkatkan keamanan
	Kurang mekanisme peman-tauan terhadap jaringan	Tingkatkan pemantauan
	Gangguan jaringan	*Maintenance*
	Kerusakan pada infrastruktur jaringan	*Maintenance*
	Kesalahan dalam melakukan konfigurasi *access Point*	*Maintenance*
	Kabel digigit oleh hewan	*Maintenance*
Karyawan (People)	Kurang training prosedur penggunaan TI yang diberikan	Dilakukan t*raining*
	Kurang sosialisasi tentang regulasi dan sanksinya	Dilakukan Sosialisasi
	Salah input dan hapus data	Dilakukan pengecekan
	Kurang mekanisme peman- tauan	Dilakukan pemantauan
	Organisasi tidak melakukan prosedur backup	Dilakukan *Backup* secara teratur

Aset	Potensi Ancaman	Penanganan
	Salah input dan hapus data	Dilakukan pengecekan
	Pembobolan data	Tingkatkan keamanan
Software: Iraise Sistem Regristasi (Sireg) Sistem Penerimaan Mahasiswa Baru (PMB)	Kurang dokumentasi	Dibuat dokumentasi
	Sistem tidak dapat di akses	Dilakukan pengecekan
	Kesalahan *coding* pada fungsional *software*	Dilakukan pengecekan
	Pembobolan data	Tingkatkan keamanan

4.5 Penentuan Kemungkinan (*Likelihood*) Sistem Akademik

Dalam menentukan kemungkinan Sistem Informasi Akademik pertama diperlukan terlebih dahulu menentukan aset yang terkait dengan Sistem Informasi Akademik UIN Suska Riau itu sendiri, kemudian aset tersebut dikelompokkan menjadi beberapa kategori. Kategori aset terdiri dari informasi, aset piranti lunak, aset fisik, layanan, dan orang. Tahapan identifikasi aset bertujuan untuk melihat kondisi aset saat ini terkait dengan manajemen keamanan informasi akademik yang ada di UIN Suska Riau. Berikut adalah nilai kemungkinan aset dari Sistem Informasi Sistem Akademik UIN Suska Riau:

Tabel 4. 7 Nilai Kemungkinan (*Likelihood*)

Kategori Aset	Nama Aset	Kode Aset	Kemungkinan	Sebutan
Informasi	Informasi Nilai Mahasiswa	IN-001	0,04243	Sangat Jarang
Perangkat Keras (*Hardware*)	Server	HD-001	0,00593	Sangat Jarang
	Komputer	HD-002	0,06972	Sangat Jarang
	Jaringan	HD-003	0,0925	Sangat Jarang
	UPS	HD-004	0,0003	Sangat Jarang
Perangkat Lunak (*Software*)	IRaise	SW-001	0,3875	Jarang
	Sistem Regristasi (Sireg)	SW-002	0,1299	Sangat Jarang
	Sistem informasi Pendaftaran Mahasiswa Baru (PMB)	SW-003	0,1204	Sangat Jarang
Karyawan	Karyawan	SDM-001	0,4	Mungkin

Sebutan yang ada pada kolom sebutan yang ada pada tabel 4.7 didapat dari tabel 2.1, untuk mendapatkan nilai probabilitas dapat diihat pada lampiran D.

Nilai Ancaman (NT) = Rerata Probabilitas x Total Kejadian

Tabel 4. 8 Tabel Perhitungan Nilai Ancaman Aset

	ID Aset: IN-001				
	Jumlah Hari: 30				
	Nama Aset: Informasi Nilai Mahasiswa				
Kejadian		**Jenis**	**Probabilitas**	**Jumlah Kejadian / 30 hari**	**Rerata Probabilitas**
Kode	**Keterangan**				
T1	Akses Ilegal (*Unauthorized Access*)	Ancaman	*Low*	2	0,0667
T3	*Hackers* (*Intruders*)	Ancaman	*Low*	1	0,0333
T6	Kebakaran (*Fire*)	Ancaman	*Low*	0	0
V1	Kerusakan Data (*Data Corruption*)	Ancaman	*Low*	0	0
V2	Kesalahan SDM (*Human Error*)	Ancaman	*Low*	8	0,2667
V5	Kesalahan Pengiriman Data (*Data Missing Recipient*)	Kelemahan	*Low*	3	0,1
V9	Tidak ada kontrol pengawasan	Kelemahan	*Low*	0	0
V10	Kurangnya tenaga ahli	Kelemahan	*Low*	0	0
Total Kejadian	8	**Jumlah Rerata Probabilitas**		14	0,4667
Nilai Ancaman (NT)					0,04243

4.6 Analisa Dampak (*Impact Analysis*) Sistem Akademik

Pada tahapan ini penulis mengajukan kuesioner berdasarkan tabel 2.2, untuk menentukan tingkatan dari suatu dampak negatif yang dihasilkan oleh sumber ancaman yang ada di Sistem Akademik UIN Suska Riau, dengan cara menganalisis dampak bisnis yang ditimbulkan oleh masing-masing aset SI/TI. Analisis dampak bisnis ini bertujuan untuk mengetahui sejauh mana dampak yang ditimbulkan dari masing-masing aset SI/TI yang terganggu oleh ancaman dan kelemahan terhadap kelangsungan bisnis dari Sistem Akademik UIN Suska Riau.

Keterangan lebih lanjut mengenai nilai dampak dapat dilihat pada tabel 4.9:

Tabel 4. 9 Analisa Dampak

No	ID Asset	Nama Asset	Dampak	Nilai
1	IN-001	Informasi Nilai Mahasiswa	Memengaruhi pencapaian beberapa sasaran / gangguan yang terjadi dapat berdampak terhadap layanan yang menggunakan sistem informasi.	5
2	HD-001	Server	Semua sasaran tidak dapat tercapai / segala kegiatan dan proses bisnis yang terhubung langsung dengan server menjadi terganggu dan tidak berjalan sesuai dengan fungsinya.	5
3	HD-002	Komputer	Memengaruhi pencapaian beberapa sasaran / aktivitas yang dilakukan menggunakan komputer menjadi terganggu, seperti halnya menginputkan data untuk keperluan bisnis tidak berjalan dengan lancar.	3
4	HD-003	UPS	Semua sasaran tidak dapat tercapai / perangkat keras yang terhubung dengan listrik dapat terjadi kerusakan atau terjadinya korsleting karena supply daya listrik tidak ada dan berpengaruh terhadap aktivitas server.	5
5	HD-004	Jaringan	Semua sasaran tidak dapat tercapai / akses internet dapat terganggu atau tidak dapat digunakan.	5
6	SW-001	IRaise	Sasaran-sasaran penting tidak dapat tercapai / mahasiswa dan dosen tidak bisa mencapai tujuan dalam penginputan data	4
7	SW-002	Sistem Regristasi (Sireg)	Memengaruhi pencapaian beberapa sasaran / mahasiswa tidak dapat melakukan regristasi	3
8	SW-003	Sistem informasi Pendaftaran Mahasiswa Baru (PMB)	Memengaruhi pencapaian beberapa sasaran / calon mahasiswa susah untuk mendapatkan informasi dan tidak bisa melakukan pendaftaran	3
9	SDM-001	Karyawan	Memengaruhi pencapaian beberapa sasaran /tidak tercapainya tujuan-tujuan secara tepat waktu	3

4.7 Penentuan Risiko (*Risk Determination*) Sistem Akademik

Pada tahap ini penulis menetapkan peringkat risiko dari yang terendah ke tertinggi, dengan cara mengalikan nilai atau tingkat dari kemungkinan dan dampak, nilai kemungkinan didapatkan dari tabel 4.7 dan tabel dampak didapatkan dari tabel 4.8, kemudian tingkat risikonya ditentukan melalui tabel matrik penilaian risiko yang dapat dilihat pada tabel 2.3. Hasil penentuan risiko dapat dilihat pada tabel 4.10.

Tabel 4. 10 Nilai Risiko

Kategori Aset	Nama Aset	Kode Aset	Kemungkinan	Dampak	Level
Informasi	Informasi Nilai Mahasiswa	IN-001	Sangat Jarang	Sangat Besar	Tinggi
Perangkat Keras (*Hardware*)	Server	HD-001	Sangat Jarang	Sangat Besar	Tinggi
	Komputer	HD-002	Sangat Jarang	Sedang	Sedang
	Jaringan	HD-003	Sangat Jarang	Sangat Besar	Tinggi
	UPS	HD-004	Sangat Jarang	Besar	Sedang
Perangkat Lunak (*Software*)	IRaise	SW-001	Jarang	Besar	Tinggi
	Sistem Regristasi (Sireg)	SW-002	Sangat Jarang	Sedang	Sedang
	Sistem informasi Pendaftaran Mahasiswa Baru (PMB)	SW-003	Sangat Jarang	Sedang	Sedang
Karyawan	Karyawan	SDM-001	Mungkin	Sedang	Sedang

4.8 Rekomendasi Kontrol Sistem Akademik

Berdasarkan ringkasan hasil penentuan level pada masing-masing kontrol keamanan yang telah dilakukan penilaian, maka dapat diberikan solusi dari hasil *assessment* tersebut berupa panduan implementasi sebagai rekomendasi dalam manajemen keamanan informasi pada masing-masing aset. Pemberian rekomendasi berdasarkan penentuan level yang telah ditentukan pada *rule-rule* rekomendasi yang telah disimpan sebelumnya di dalam data master. Rekomendasi dapat dikembangkan dengan menambah data rekomendasi dan data *rule* rekomendasi pada data master.

Berdasarkan hasil proses identifikasi risiko aset-aset SI/TI Sistem Akademik UIN Suska Riau maka dapat diberikan solusi berupa kriteria penerimaan risiko aset dan rekomendasi penanganan dari ancaman dan kelemahan yang mungkin diterima oleh masing-masing aset SI/TI. Penentuan rekomendasinya dapat dilihat pada tabel 2.4, tabel matriks kriteria penerimaan risiko merupakan hubungan antara variabel berikut : Probabilitas Ancaman (PA) yang didapat dari perhitungan pada Lampiran D, Biaya Pemulihan (BP) akibat atau dampak dari penerimaan risiko yang didapat dari hasil wawancara, dan Biaya

Transfer Risiko (BR) kepada pihak ketiga yang didapat dari hasil wawancara. Berikut adalah rekomendasi untuk ancaman dari risiko Sistem Akademik dapat dilihat pada tabel 4. 11:

Tabel 4. 11 Hasil Rekomendasi

NO	Nama Aset	BP	BR	PA	Kriteria
1	Informasi Nilai Mahasiswa	LOW	HIGH	LOW	*Risk Acceptance*
2	Server	LOW	HIGH	LOW	*Risk Acceptance*
3	Komputer	LOW	HIGH	LOW	*Risk Acceptance*
4	Jaringan	MED	MED	LOW	*Risk Reduction*
5	UPS	MED	MED	LOW	*Risk Reduction*
6	IRaise	MED	MED	MED	*Risk Reduction*
7	Sistem Regristasi (Sireg)	LOW	HIGH	LOW	*Risk Acceptance*
8	Sistem informasi Pendaftaran Mahasiswa Baru (PMB)	LOW	HIGH	LOW	*Risk Acceptance*
9	Karyawan	HIGH	LOW	MED	*Risk Transfer*

4.9 Dokumentasi Hasil Kegiatan Penilaian Risiko

Hasil dari kegiatan penilaian risiko dari sistem akademik adalah dari 9 aset yang telah ditentukan berhubungan langsung dengan sistem akademik, setelah dilakukan penilaian risiko didapatlah hasil sebagai berikut :

1. Lima (5) risiko level sedang yaitu Komputer, UPS, Karyawan, Sistem Informasi Pendaftaran Mahasiswa Baru (PMB) dan Sistem Regristasi (Sireg).
2. Empat (4) risiko level tinggi yaitu : Iraise, Server, Jaringan dan Informasi Nilai Mahasiswa.

Setelah didapatkan level risiko ditetapkan rekomendasi untuk diterapkan oleh organisai, rekomendasi didapatkan dari probabilitas ancaman (*threat probability*), biaya pemulihan (*recovery cost*) akibat atau dampak dari penerimaan risiko, dan biaya transfer risiko (*risk transfer cost*) kepada pihak ketiga. Rekomendasi untuk setiap asset dapat dilihat pada tabel 4.11, informasi nilai

mahasiswa, server, komputer, Sireg, dan PMB mendapatkan rekomendasi *Risk Acceptance*. UPS, IRAISE, dan jaringan memiliki rekomendasi *Risk Reduction*. Sedangkan karyawan mendapatkan rekomendasi *Risk Transfer*.

4.10 Analisa dan Perancangan Sistem Penilaian Risiko Keamanan Informasi

Pada analisa dan perancangan Sistem Penilaian Risiko Keamanan Informasi membahas mengenai analisa kebutuhan data, analisa fungsional sistem, dan perancangan sistem.

4.10.1 Analisa Kebutuhan Data

Analisis kebutuhan data diperlukan sebelum melakukan peracangan sistem informasi yang akan dibuat karena sistem membutuhkan data berupa masukan (*input*) agar dapat diolah pada sistem untuk menghasilkan data keluaran (*output*) yang sesuai dengan yang diharapkan.

A. Data Masukan

Data masukan yang dibutuhkan pada Sistem Penilaian menggunakan NIST SP 800-30 adalah data master yang terdiri dari data aset, data ancaman, data instansi, data kemungkinan dan data dampak. Berikut adalah penjelasannya:

1. Data Instansi

   Data Instansi merupakan data yang berisi tentang informasi instansi yang melakukan penilaian risiko.

2. Data Aset

   Data aset merupakan merupakan data yang berisi daftar aset yang dimiliki oleh UIN Suska Riau khususnya aset yang berhubungan langsung dengan Sistem Akademik Di UIN Suska Riau yaitu Informasi, perangkat keras, dan perangkat lunaknya.

3. Data Ancaman

   Data ancaman merupakan data yang berisi daftar ancaman yang relevan dengan aset yang dikelola.

4. Data kemungkinan

Data kemungkinan merupakan data yang berisi tingkatan kemungkinan terjadinya suatu ancaman yang diisi oleh pihak organisasi.

5. Data Dampak

   Data Dampak merupakan data yang berisi informasi seberapa pentingnya aset tingkatan dampaknya terhadap jalan proses bisnis organisasi.

B. Proses

Proses pengolahan data yang ada pada Sistem Informasi Penilaian Risiko Keamanan Informasi Sistem Akademik UIN Suska Riau adalah sebagai berikut:

1. *Login*

   Proses *login* ini digunakan untuk mengenali pengguna yang sah sesuai dengan *username* dan *password* yang telah terdaftar pada sistem.

2. Pengelolaan Data Master

   Proses pengelolaan data master adalah proses memasukan data yang akan diproses pada sistem yang dibuat. Data yang dimasukkan yaitu data master instansi, aset, data ancaman, data kemungkinan, dan data dampak.

3. *Risk Assestment Test*

   Proses *risk assessment test* adalah proses penilaian risiko berdasarkan kemungkianan dan dampak yang dikalikan.

4. Hasil Uji

   Hasil uji merupakan proses menampilkan *risk assessment test* yang telah dilakukan. Pada proses ini auditor menginputkan nilai kemungkinan setiap ancaman berdasarkan kemungkinan terjadinya yang telah diberikan skala tingkatannya.

C. Data Keluaran

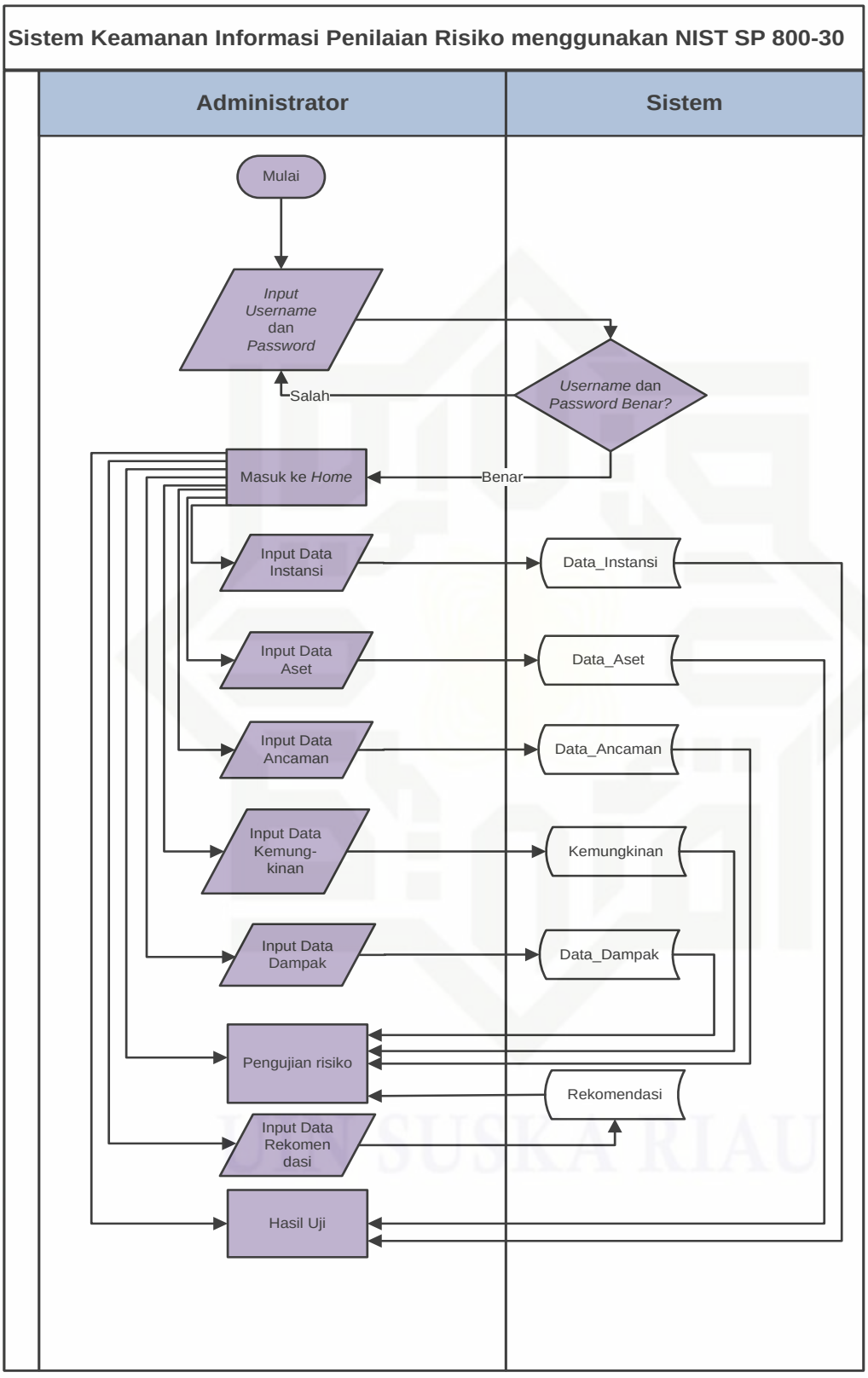
Data keluaran *(output)* yang akan ditampilkan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan Metode NIST SP 800-30 berupa laporan hasil penilaian risiko aset yang berisi informasi mengenai tingkatan nilai risiko.

4.10.2 Analisa Fungsional Sistem

Pada tahap analisa fungsional sistem akan dijelaskan mengenai perancangan Sistem Penilaian Risiko Keamanan Informasi menggunakan Metode NIST SP 800-30 dengan menggunakan UML (*Unified Modeling Language*). Analisa fungsional sistem pada penelitian ini terdiri dari *Flowchart, use case diagram, sequence diagram, deployment diagram,* dan *database.*

A. *Flowchart*

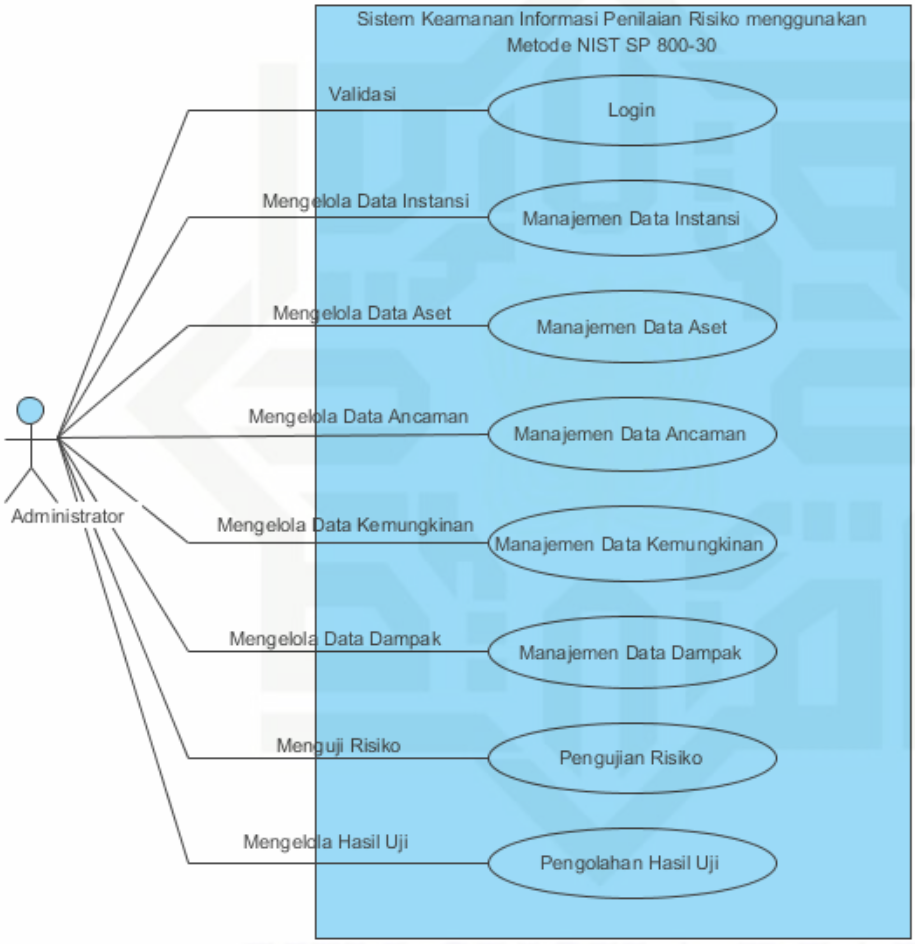
Flowchart diagram berfungsi untuk menjelaskan alur dari sistem dari mulai sampai selesai. Berikut ini adalah *flowchart* Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 2 *Flowchart Diagram*

B. *Use Case Diagram*

Use case diagram berfungsi untuk mengetahui fungsi apa saja yang ada dalam sebuah sistem dan siapa saja yang berhak atau boleh menggunakan sistem tersebut. *Use case diagram* juga berguna untuk menjelaskan ruang lingkup sistem. Berikut adalah *Use Case Diagram* Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 3 *Use Case Diagram*

C. *Use Case* Spesifikasi

Use Case Spesifikasi berfungsi untuk menjelaskan setiap proses pada *use case diagram*, *Use Case* Spesifikasi juga bisa disebut sebagai penjelas alur pada setiap proses sistem informasi. Berikut adalah tabel-tabel spesifikasi *use case* pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30 dapat dilihat dipenjelasan tabel berikut:

1. Spesifikasi *Use Case Login*

Spesifikasi *use case login* menunjukan kondisi dari proses masuk akun pengguna ke sistem oleh pengguna. Berikut tabel *use case login*:

Tabel 4. 12 Spesifikasi *Use case Login*

Nama	***Use Case Login***
Deskripsi	*Use case login* memungkinkan pengguna untuk mengakses sistem.
Aktor Utama	*Administrator*
Kondisi Awal	*Username* dan *Password* pengguna telah terdaftar sebagai akun.
Kodisi Akhir	Pengguna masuk ke sistem dan ditampilkan menu *home*.
Skenario Utama	1. Pengguna membuka halaman *login* pengguna. 2. Sistem menampilkan halaman *login* pengguna. 3. Pengguna mengisikan *Username* dan *password*. 4. Pengguna menekan tombol *login*. 5. Sistem memvalidasi akun pengguna. 6. Sistem menampilkan halaman awal pengguna.
Alternatif Skenario	Jika username atau password tidak sesuai maka sistem akan menampilkan pesan email atau password salah.

2. Spesifikasi *Use Case* Manajemen Data Instansi

Spesifikasi *use case* manajemen data instansi berfungsi untuk menunjukan kondisi dari proses pengolahan data instansi oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut tabel spesifikasi *use case* manajemen data instansi:

a. Spesifikasi *Use Case* Tambah Data Instansi

Spesifikasi *use case* tambah data instansi berfungsi untuk menunjukkan proses penambahan data instansi. Berikut adalah spesifikasi *use case* tambah data instansi:

Tabel 4. 11 Spesifikasi *Use Case* Tambah Data Instansi

Nama	***Use Case* Tambah Data Instansi**
Deskripsi	*Use case* tambah data instansi memungkinkan *administrator* untuk menambah data instansi.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data instansi
Kodisi Akhir	Data instansi tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menambah data instansi. 2. *Administrator* memilih pilihan menu data instansi. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol tambah. 4. *Administrator* meng-*submit* data instansi. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

b. Spesifikasi *Use Case* Ubah Data Instansi

Spesifikasi *use case* ubah data instansi berfungsi untuk menunjukkan proses pengubahan data instansi. Berikut adalah spesifikasi *use case* ubah data instansi:

Tabel 4. 12 Spesifikasi *Use Case* Ubah Data Instansi

Nama	***Use Case* Ubah Data Instansi**
Deskripsi	*Use case* ubah data instansi memungkinkan *administrator* untuk mengubah data instansi.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data instansi
Kodisi Akhir	Perubahan data instansi tersimpan

Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin mengubah data instansi. 2. *Administrator* memilih pilihan menu data instansi. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol ubah. 4. *Administrator* meng-*submit* data instansi yang akan dirubah. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

c. Spesifikasi *Use Case* Hapus Data Instansi

Spesifikasi *use case* hapus data instansi berfungsi untuk menunjukkan proses penghapusan data instansi. Berikut adalah spesifikasi *use case* hapus data instansi:

Tabel 4. 13 Spesifikasi *Use Case* Hapus Data Instansi

Nama	***Use Case* Hapus Data Instansi**
Deskripsi	*Use case* hapus data instansi memungkinkan *administrator* untuk menghapus data instansi.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data instansi
Kodisi Akhir	Data terhapus
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menghapus data instansi. 2. *Administrator* memilih pilihan menu data instansi. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol hapus. 4. *Administrator* menenakan ya.
Alternatif Skenario	-

3. Spesifikasi *Use Case* Manajemen Data Aset

Spesifikasi *use case* manajemen data aset berfungsi untuk menunjukan kondisi dari proses pengolahan data aset oleh *administrato*r, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut tabel spesifikasi *use case* manajemen data aset:

a. Spesifikasi *Use Case* Tambah Data Aset

Spesifikasi *use case* tambah data aset berfungsi untuk menunjukkan proses penambahan data aset. Berikut adalah spesifikasi *use case* tambah data aset:

Tabel 4. 16 Spesifikasi *Use Case* Tambah Data Aset

Nama	***Use Case* Tambah Data aset**
Deskripsi	*Use case* tambah data aset memungkinkan *administrator* untuk menambah data aset.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data aset
Kodisi Akhir	Data aset tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menambah data aset. 2. *Administrator* memilih pilihan menu data aset. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol tambah. 4. *Administrator* meng-*submit* data aset. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

b. Spesifikasi *Use Case* Ubah Data Aset

Spesifikasi *use case* ubah data aset berfungsi untuk menunjukkan proses pengubahan data aset. Berikut adalah spesifikasi *use case* ubah data aset:

Tabel 4. 17 Spesifikasi *Use Case* Ubah Data Aset

Nama	***Use Case* Ubah Data Aset**
Deskripsi	*Use case* ubah data aset memungkinkan *administrator* untuk mengubah data aset.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data aset

Kodisi Akhir	Perubahan data aset tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin mengubah data aset. 2. *Administrator* memilih pilihan menu data aset. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol ubah. 4. *Administrator* meng-*submit* data aset yang akan dirubah. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

c. Spesifikasi *Use Case* Hapus Data Aset

Spesifikasi *use case* hapus data aset berfungsi untuk menunjukkan proses penghapusan data aset. Berikut adalah spesifikasi *use case* hapus data aset:

Tabel 4. 18 Spesifikasi *Use Case* Hapus Data Aset

Nama	***Use Case* Hapus Data Aset**
Deskripsi	*Use case* hapus data aset memungkinkan *administrator* untuk menghapus data aset.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data aset
Kodisi Akhir	Data terhapus
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menghapus data aset. 2. *Administrator* memilih pilihan menu data aset. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol hapus. 4. *Administrator* menenakan ya.

4. Spesifikasi *Use Case* Manajemen Data Ancaman

Spesifikasi *use case* manajemen data ancaman berfungsi untuk menunjukan kondisi dari proses pengolahan data ancaman oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut tabel spesifikasi *use case* manajemen data ancaman:

a. Spesifikasi *Use Case* Tambah Data Ancaman

Spesifikasi *use case* tambah data ancaman berfungsi untuk menunjukkan proses penambahan data ancaman. Berikut adalah spesifikasi *use case* tambah data ancaman:

Tabel 4. 19 Spesifikasi *Use Case* Tambah Data Ancaman

Nama	***Use Case* Tambah Data Ancaman**
Deskripsi	*Use case* tambah data ancaman memungkinkan *administrator* untuk menambah data ancaman.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data ancaman
Kodisi Akhir	Data ancaman tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menambah data ancaman. 2. *Administrator* memilih pilihan menu data ancaman. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol tambah. 4. *Administrator* meng-*submit* data ancaman. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

b. Spesifikasi *Use Case* Ubah Data Ancaman

Spesifikasi *use case* ubah data ancaman berfungsi untuk menunjukkan proses pengubahan data ancaman. Berikut adalah spesifikasi *use case* ubah data ancaman:

Tabel 4. 20 Spesifikasi *Use Case* Ubah Data Ancaman

Nama	***Use Case* Ubah Data Ancaman**
Deskripsi	*Use case* ubah data ancaman memungkinkan *administrator* untuk mengubah data ancaman.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data ancaman
Kodisi Akhir	Perubahan data ancaman tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin mengubah data ancaman. 2. *Administrator* memilih pilihan menu data ancaman. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol ubah. 4. *Administrator* meng-*submit* data ancaman yang akan dirubah. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

c. Spesifikasi *Use Case* Hapus Data Ancaman

Spesifikasi *use case* hapus data ancaman berfungsi untuk menunjukkan proses penghapusan data ancaman. Berikut adalah spesifikasi *use case* hapus data ancaman:

Tabel 4. 21 Spesifikasi *Use Case* Hapus Data Ancaman

Nama	***Use Case* Hapus Data Ancaman**
Deskripsi	*Use case* hapus data ancaman memungkinkan *administrator* untuk menghapus data ancaman.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data ancaman
Kodisi Akhir	Data terhapus
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menghapus data ancaman.

	2. *Administrator* memilih pilihan menu data ancaman. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol hapus. 4. *Administrator* menenakan ya.
Alternatif Skenario	-

5. Spesifikasi *Use Case* Manajemen Data Kemungkinan

Spesifikasi *use case* manajemen data kemungkinan berfungsi untuk menunjukan kondisi dari proses pengolahan data kemungkinan oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Untuk lebih jelas lagi berikut tabel spesifikasi *use case* manajemen data kemungkinan:

a. Spesifikasi *Use Case* Tambah Data Kemungkinan

Spesifikasi *use case* tambah data kemungkinan berfungsi untuk menunjukkan proses penambahan data kemungkinan. Berikut adalah spesifikasi *use case* tambah data kemungkinan:

Tabel 4. 22 Spesifikasi *Use Case* Tambah Data Kemungkinan

Nama	***Use Case* Tambah Data Kemungkinan**
Deskripsi	*Use case* tambah data kemungkinan memungkinkan *administrator* untuk menambah data kemungkinan.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data kemungkinan
Kodisi Akhir	Data kemungkinan tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menambah data kemungkinan. 2. *Administrator* memilih pilihan menu data kemungkinan. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol tambah. 4. *Administrator* meng-*submit* data kemungkinan. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

b. Spesifikasi *Use Case* Ubah Data Kemungkinan

Spesifikasi *use case* ubah data kemungkinan berfungsi untuk menunjukkan proses pengubahan data kemungkinan. Berikut adalah spesifikasi *use case* ubah data kemungkinan:

Tabel 4. 23 Spesifikasi *Use Case* Ubah Data Kemungkinan

Nama	***Use Case* Ubah Data Kemungkinan**
Deskripsi	*Use case* ubah data kemungkinan memungkinkan *administrator* untuk mengubah data kemungkinan.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data kemungkinan
Kodisi Akhir	Perubahan data kemungkinan tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin mengubah data kemungkinan. 2. *Administrator* memilih pilihan menu data kemungkinan. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol ubah. 4. *Administrator* meng-*submit* data kemungkinan yang akan dirubah. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

c. Spesifikasi *Use Case* Hapus Data Kemungkinan

Spesifikasi *use case* hapus data kemungkinan berfungsi untuk menunjukkan proses penghapusan data kemungkinan. Berikut adalah spesifikasi *use case* hapus data kemungkinan:

Tabel 4. 24 Spesifikasi *Use Case* Hapus Data Kemungkinan

Nama	***Use Case* Hapus Data Kemungkinan**
Deskripsi	*Use case* hapus data kemungkinan memungkinkan *administrator* untuk menghapus data kemungkinan.
Aktor Utama	*Administrator*

Kondisi Awal	Sistem menampilkan halaman data kemungkinan
Kodisi Akhir	Data terhapus
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menghapus data kemungkinan. 2. *Administrator* memilih pilihan menu data kemungkinan. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol hapus. 4. *Administrator* menenakan ya.
Alternatif Skenario	-

6. Spesifikasi *Use Case* Manajemen Data Dampak

Spesifikasi *use case* manajemen data dampak berfungsi untuk menunjukan kondisi dari proses pengolahan data dampak oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut tabel spesifikasi *use case* manajemen data dampak:

a. Spesifikasi *Use Case* Tambah Data Dampak

Spesifikasi *use case* tambah data dampak berfungsi untuk menunjukkan proses penambahan data dampak. Berikut adalah spesifikasi *use case* tambah data dampak:

Tabel 4. 25 Spesifikasi *Use Case* Tambah Data Dampak

Nama	***Use Case* Tambah Data Dampak**
Deskripsi	*Use case* tambah data dampak memungkinkan *administrator* untuk menambah data dampak.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data dampak
Kodisi Akhir	Data dampak tersimpan

Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menambah data dampak. 2. *Administrator* memilih pilihan menu data dampak. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol tambah. 4. *Administrator* meng-*submit* data dampak. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

b. Spesifikasi *Use Case* Ubah Data Dampak

Spesifikasi *use case* ubah data dampak berfungsi untuk menunjukkan proses pengubahan data dampak. Berikut adalah spesifikasi *use case* ubah data dampak:

Tabel 4. 26 Spesifikasi *Use Case* Ubah Data Dampak

Nama	***Use Case* Ubah Data Dampak**
Deskripsi	*Use case* ubah data dampak memungkinkan *administrator* untuk mengubah data dampak.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data dampak
Kodisi Akhir	Perubahan data dampak tersimpan
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin mengubah data dampak. 2. *Administrator* memilih pilihan menu data dampak. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol ubah. 4. *Administrator* meng-*submit* data dampak yang akan dirubah. 5. *Administrator* menekan tombol *submit*.
Alternatif Skenario	Jika salah satu data tidak diisi, sistem menampilkan peringatan data harus diisi.

c. Spesifikasi *Use Case* Hapus Data Dampak

Spesifikasi *use case* hapus data dampak berfungsi untuk menunjukkan proses penghapusan data dampak. Berikut adalah spesifikasi *use case* hapus data dampak:

Tabel 4. 27 Spesifikasi *Use Case* Hapus Data Dampak

Nama	***Use Case* Hapus Data Dampak**
Deskripsi	*Use case* hapus data dampak memungkinkan *administrator* untuk menghapus data dampak.
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman data dampak
Kodisi Akhir	Data terhapus
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menghapus data dampak. 2. *Administrator* memilih pilihan menu data dampak. 3. *Administrator* memilih satu dari salah satu tombol yang disediakan (tambah, ubah, dan hapus) yaitu tombol hapus. 4. *Administrator* menenakan ya.
Alternatif Skenario	-

7. Spesifikasi *Use Case* Pengujian Risiko

Spesifikasi *use case* pengujian risiko berguna untuk menjelaskan bagaimana *administrator* melakukan aksi pengujian risiko. Berikut tabel spesifikasi *use case* pengujian risiko:

Tabel 4. 28 Spesifikasi *Use Case* Pengujian Risiko

Nama	***Use Case* Pengujian Risiko**
Deskripsi	*Use case* pengujian risiko memungkinkan
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman pengujian risiko
Kodisi Akhir	Tingkatan nilai risiko pada setiap aset
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* akan melakukan pengujian risiko. 2. *Administrator* memilih instansi.

	3. *Administrator* mengisi nilai kemungkinan pada setiap ancaman di setiap asetnya. 4. *Administrator* mengisi data dampak. 5. Nilai risi pada setiap aset keluar.
Alternatif Skenario	-

8. Spesifikasi *Use Case* Hasil Uji

Spesifikasi *use case* hasil uji berguna untuk menjelaskan bagaimana *administrator* melakukan melihat hasil dari pengujian risiko. Berikut tabel spesifikasi *use case* hasil uji:

Tabel 4. 29 Spesifikasi *Use Case* Hasil Uji

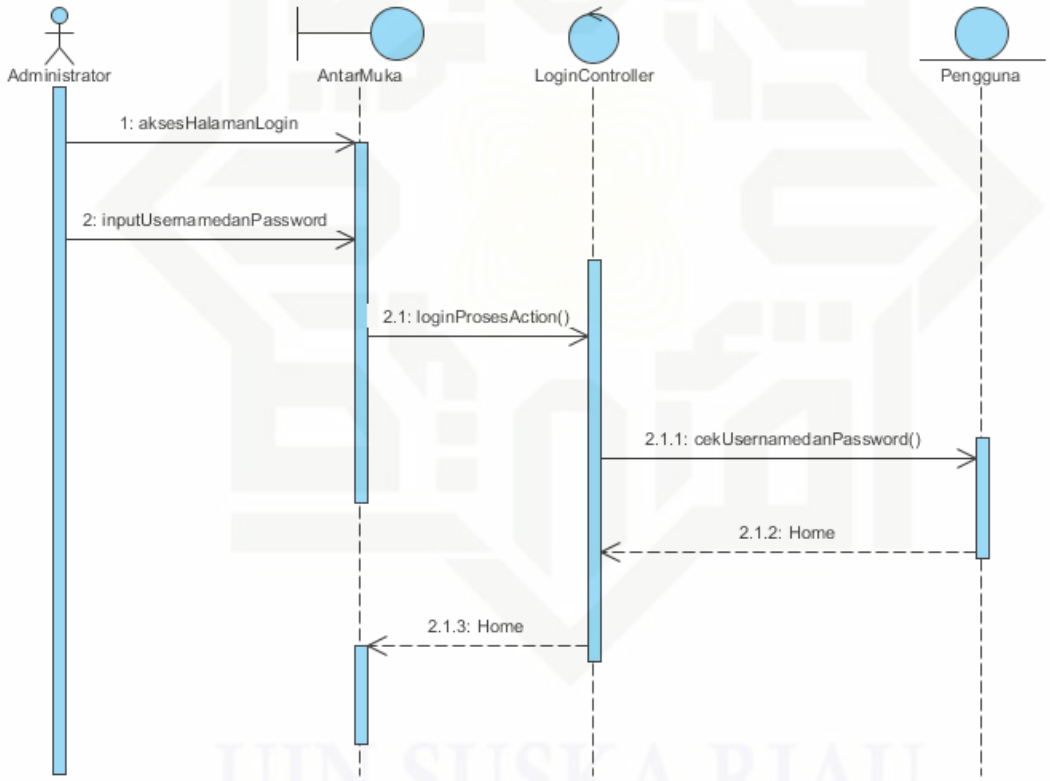
Nama	***Use Case* Hasil Uji**
Deskripsi	*Use case* hasil uji
Aktor Utama	*Administrator*
Kondisi Awal	Sistem menampilkan halaman manajemen hasil uji
Kodisi Akhir	Menampilkan data hasil uji
Skenario Utama	1. *Use case* ini dimulai ketika *administrator* ingin menampilkan hasil uji dari pengujian risiko. 2. *Administrator* memilih pilihan menu hasil uji. 3. *Administrator* menekan *check* pada salah satu hasil uji. 4. *Administrator* menekan *detail* untuk melihat *detail* hasil uji
Alternatif Skenario	-

D. *Sequence Diagram*

Sequence diagram menggambarkan hubungan antar objek pada sistem, oleh karena itu untuk membuat sebuah *sequence diagram* harus memahami objek yang terlibat. *Sequence diagram* juga menggambarkan rangkaian langkah yang dilakukan untuk menghasilkan suatu *output*. Oleh karena itu, untuk membuat suatu *sequence diagram* harus memahami objek yang terlibat serta metode yang digunakan. *Sequence diagram* yang dibuat minimal sebanyak *use case* yang ada. Untuk lebih jelas lagi berikut adalah *sequence diagram* pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30 dapat dilihat dipenjelasan dan gambar berikut ini:

1. *Sequence Diagram Login*

Proses ini dimulai ketika *administrator* ingin masuk ke Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. *Administrator* mengakses *link* Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30, sistem menampilkan halaman *login*. Kemudian pengguna memasukkan *username* dan *password*, lalu menekan tombol *login*. Setelah itu *controller* memeriksa *username* dan *password* ke tabel pengguna, jika sesuai maka *controller* akan menampilkan tampilan utama *administrator*. Berikut adalah *sequence diagram login* :



Gambar 4. 4 *Sequence Diagram Login*

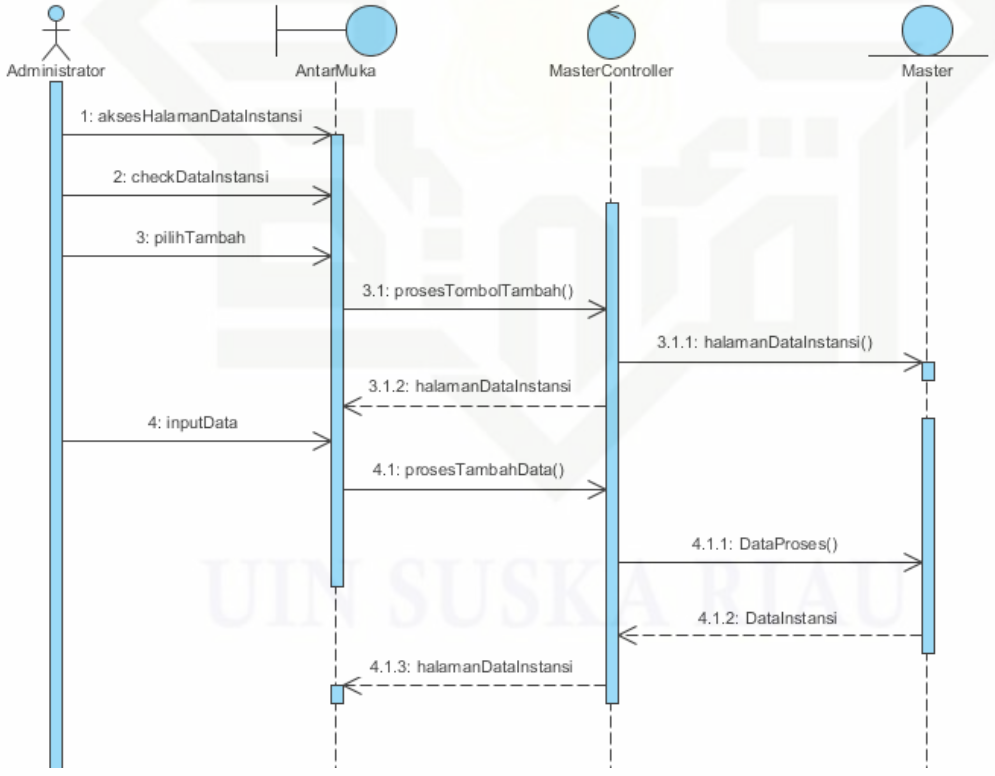
2. *Sequence Diagram* Manajemen Data Instansi

Sequence diagram manajemen data Instansi berfungsi untuk menunjukan kondisi dari proses pengolahan data instansi oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut adalah

Sequence diagram dari masing-masing proses yang ada di manajemen instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

a. *Sequence diagram* tambah data instansi

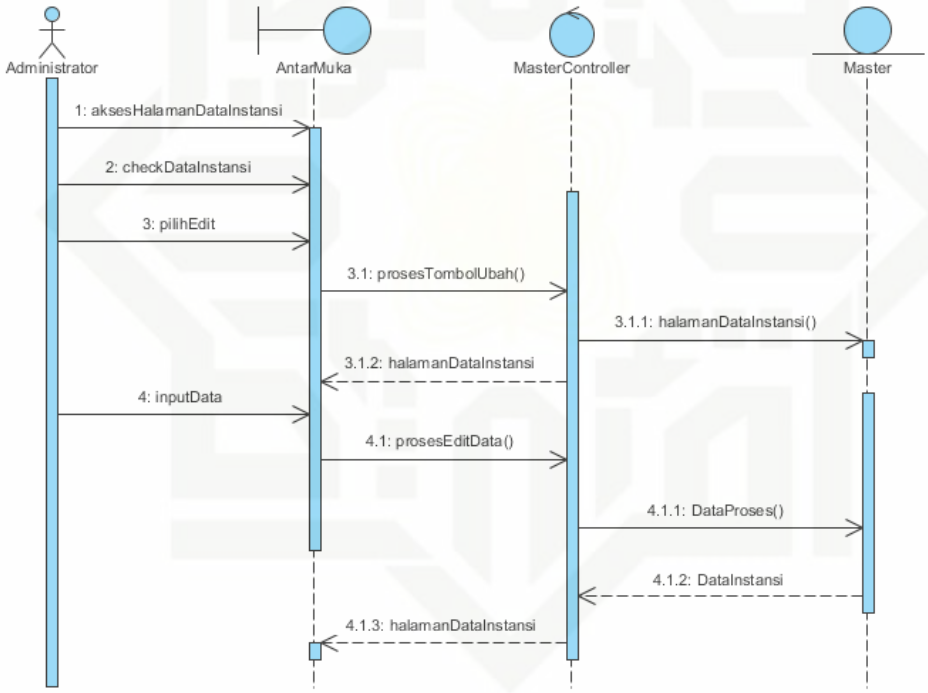
Proses tambah dimulai dari saat *administrator* ingin menambah data instansi. Pertama *administrator* mengakses halaman data instansi kemudian *check* pada data instansi yang akan ditambah lalu *administrator* menekan tombol tambah instansi, setelah itu *controller* memproses proses tambah dan menampilkan halaman tambah instansi, lalu *administrator* mengisi data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* tambah data instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 5 *Sequence Diagram* Tambah Data Instansi

b. *Sequence diagram* ubah data instansi

Proses ubah dimulai dari saat *administrator* ingin merubah data instansi. Pertama *administrator* mengakses halaman data instansi kemudian *check* pada data instansi yang akan dirubah lalu *administrator* menekan tombol *edit*, setelah itu *controller* memproses proses edit dan menampilkan halaman *edit* data instansi, lalu *administrator* mengisi data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* ubah data instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

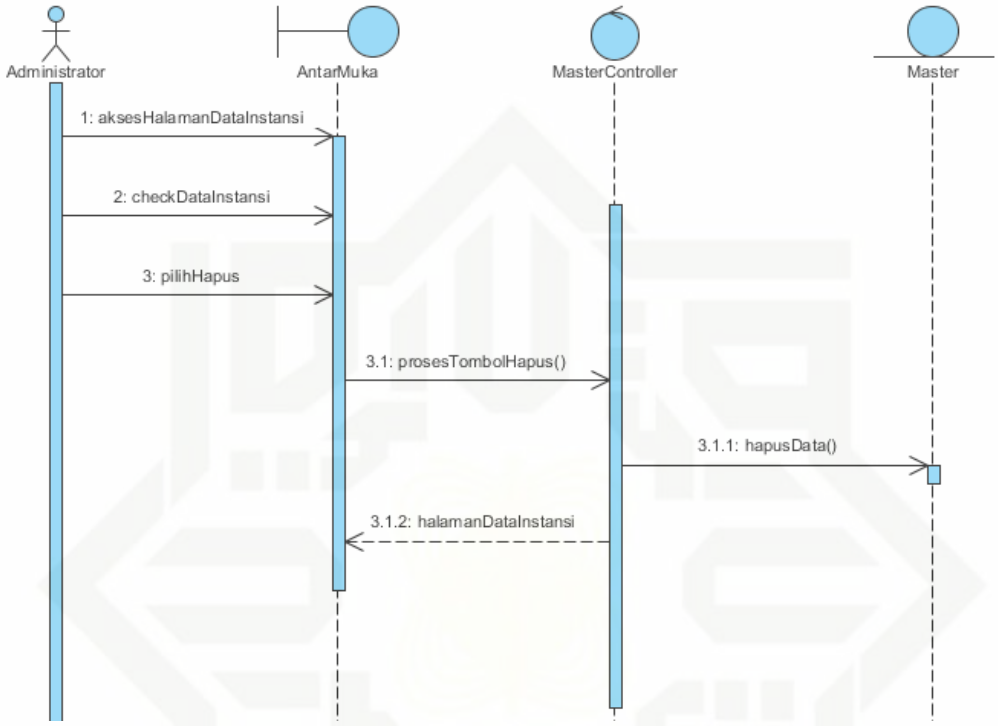


Gambar 4. 6 *Sequence Diagram* Ubah Data Instansi

c. *Sequence diagram* hapus data instansi

Proses hapus data instansi dimulai dari saat *administrator* ingin menghapus data instansi. Pertama *administrator* mengakses halaman data instansi kemudian *check* pada data instansi yang akan dihapus lalu *administrator* menekan tombol hapus, setelah itu *controller* memproses proses hapu dan menampilkan halaman data instansi.

Untuk lebih jelas lagi berikut adalah *sequence diagram* hapus data instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 7 *Sequence Diagram* Hapus Data Instansi

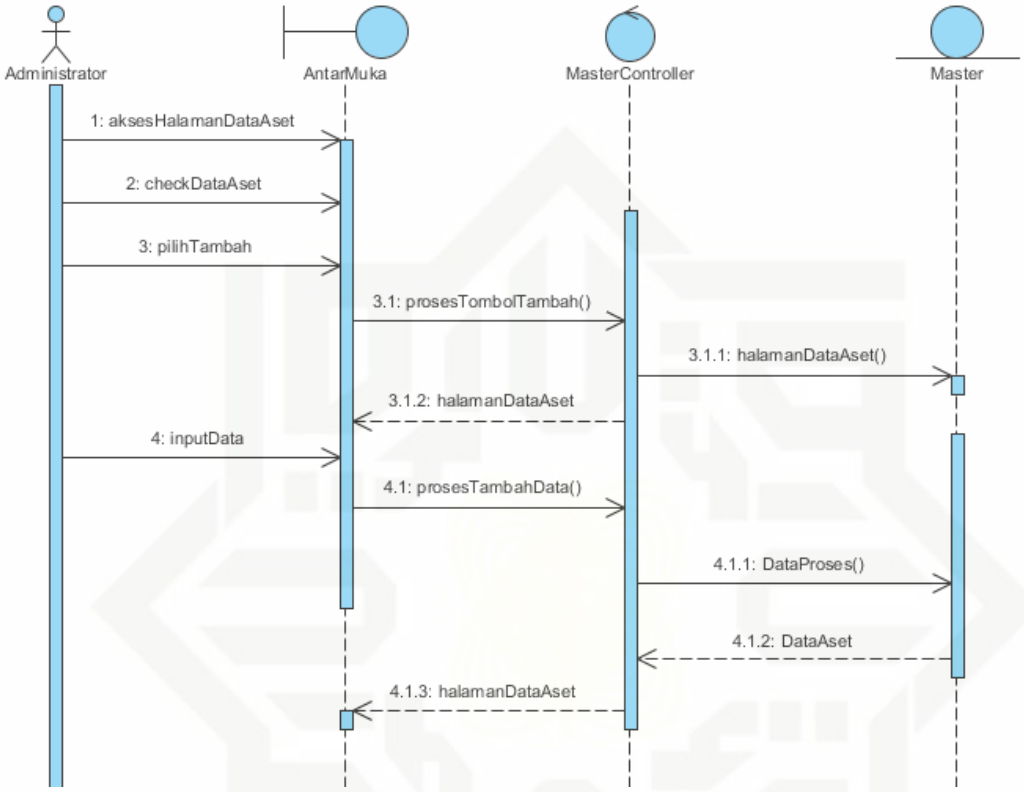
3. *Sequence Diagram* Manajemen Aset

Sequence diagram manajemen data aset berfungsi untuk menunjukan kondisi dan alur dari proses pengolahan data aset oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut adalah *Sequence diagram* dari masing-masing proses yang ada di manajemen aset pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

a. *Sequence diagram* tambah data aset

Proses tambah dimulai dari saat *administrator* ingin menambah data aset. Pertama *administrator* mengakses halaman data aset kemudian *check* pada data aset yang akan ditambah lalu *administrator* menekan tombol tambah aset, setelah itu *controller* memproses proses tambah dan menampilkan halaman tambah aset, lalu *administrator* mengisi

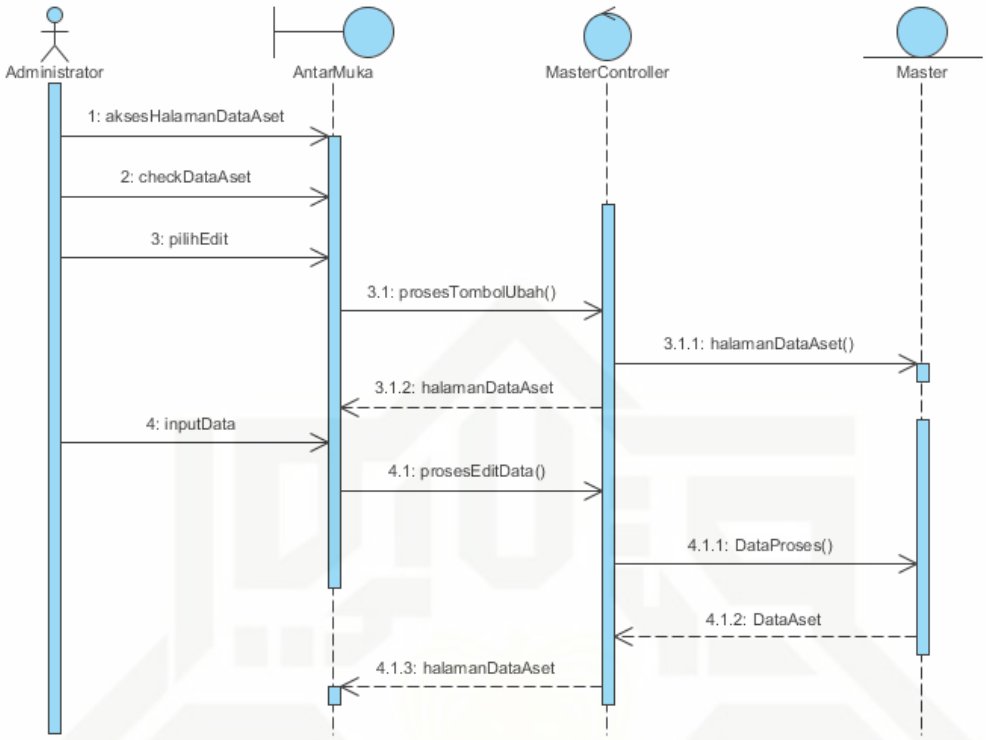
data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* tambah data aset pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 8 *Sequence Diagram* Tambah Data Aset

b. *Sequence diagram* ubah data aset

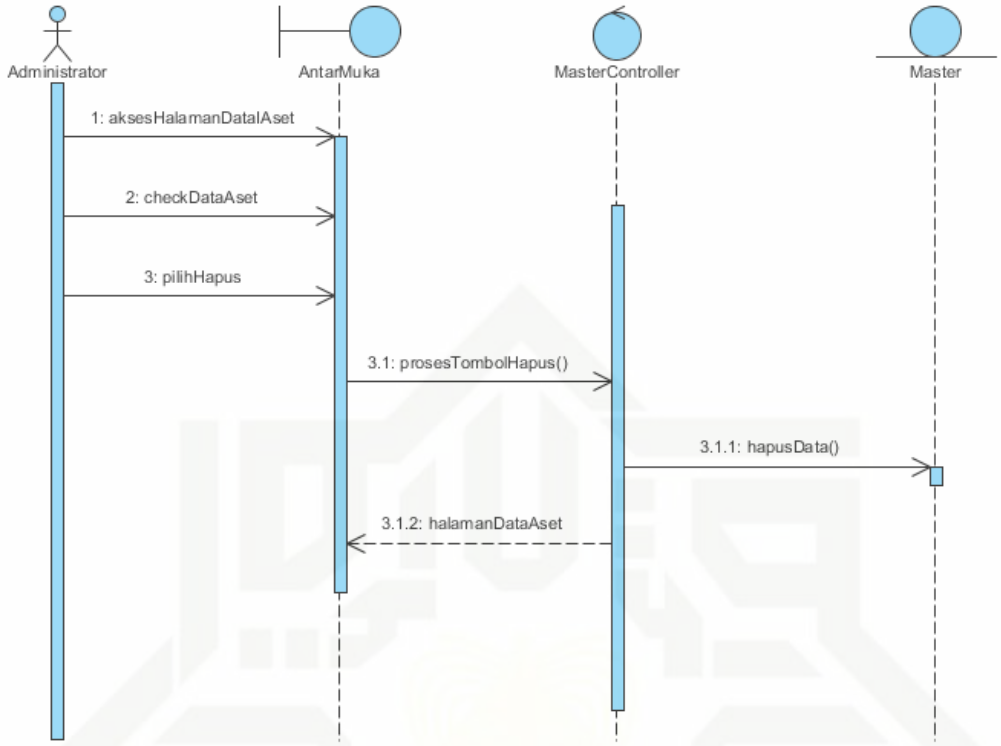
Proses ubah dimulai dari saat *administrator* ingin merubah data aset. Pertama *administrator* mengakses halaman data aset kemudian *check* pada data aset yang akan dirubah lalu *administrator* menekan tombol *edit*, setelah itu *controller* memproses proses edit dan menampilkan halaman *edit* data aset, lalu *administrator* mengisi data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* ubah data aset pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 9 *Sequence Diagram* Ubah Data Aset

c. *Sequence diagram* hapus data aset

Proses hapus data aset dimulai dari saat *administrator* ingin menghapus data aset. Pertama *administrator* mengakses halaman data aset kemudian *check* pada data aset yang akan dihapus lalu *administrator* menekan tombol hapus, setelah itu *controller* memproses proses hapu dan menampilkan halaman data aset. Untuk lebih jelas lagi berikut adalah *sequence diagram* hapus data aset pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 10 *Sequence Diagram* Hapus Data Aset

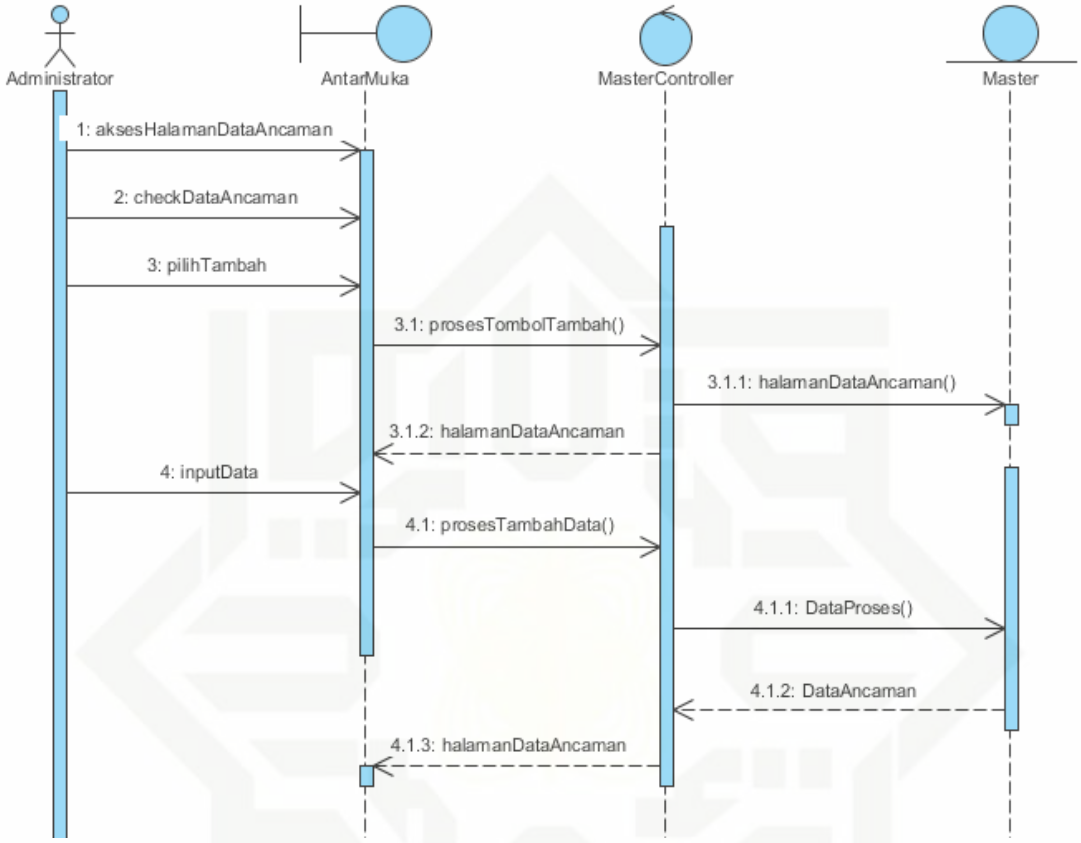
4. *Sequence Diagram* Manajemen Ancaman

Sequence diagram manajemen data ancaman berfungsi untuk menunjukan kondisi dan alur dari proses pengolahan data ancaman oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut adalah *Sequence diagram* dari masing-masing proses yang ada di manajemen ancaman pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

a. *Sequence diagram* tambah data ancaman

Proses tambah dimulai dari saat *administrator* ingin menambah data ancaman. Pertama *administrator* mengakses halaman data ancaman kemudian *check* pada data ancaman yang akan ditambah lalu *administrator* menekan tombol tambah ancaman, setelah itu *controller* memproses proses tambah dan menampilkan halaman tambah ancaman, lalu *administrator* mengisi data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* tambah data

ancaman pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

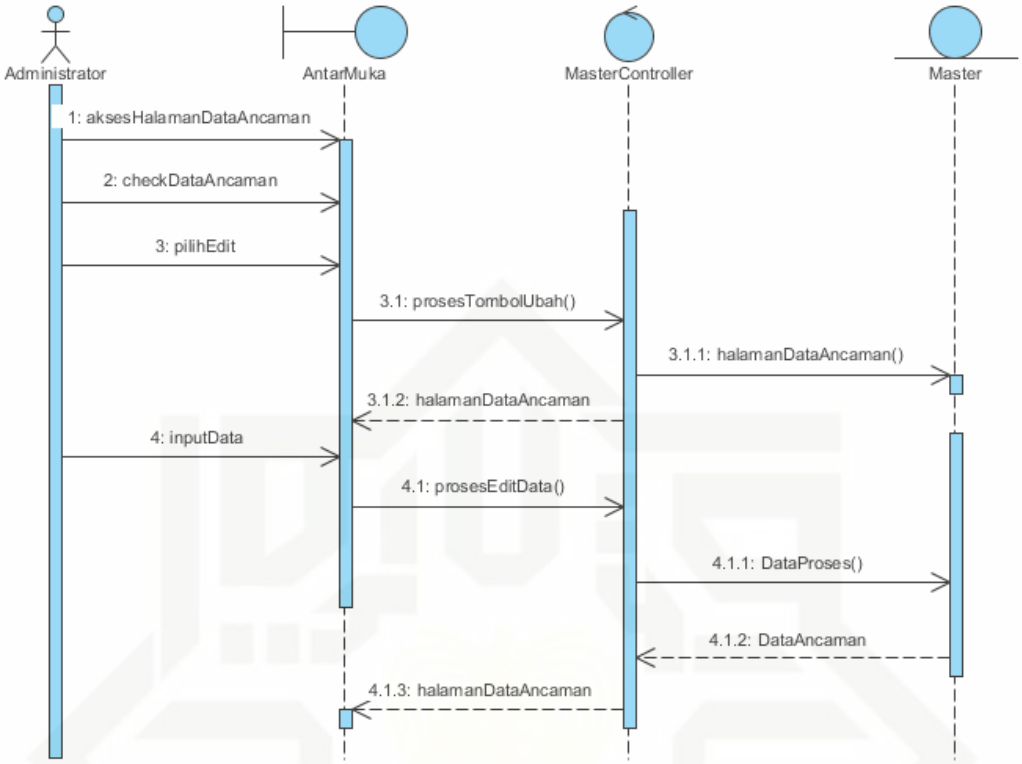


Gambar 4. 11 *Sequence Diagram* Tambah Data Ancaman

b. *Sequence diagram* ubah data ancaman

Proses ubah dimulai dari saat *administrator* ingin merubah data ancaman. Pertama *administrator* mengakses halaman data ancaman kemudian *check* pada data ancaman yang akan dirubah lalu *administrator* menekan tombol *edit*, setelah itu *controller* memproses proses edit dan menampilkan halaman *edit* data ancaman, lalu *administrator* mengisi data dan menekan tombol *submit*.

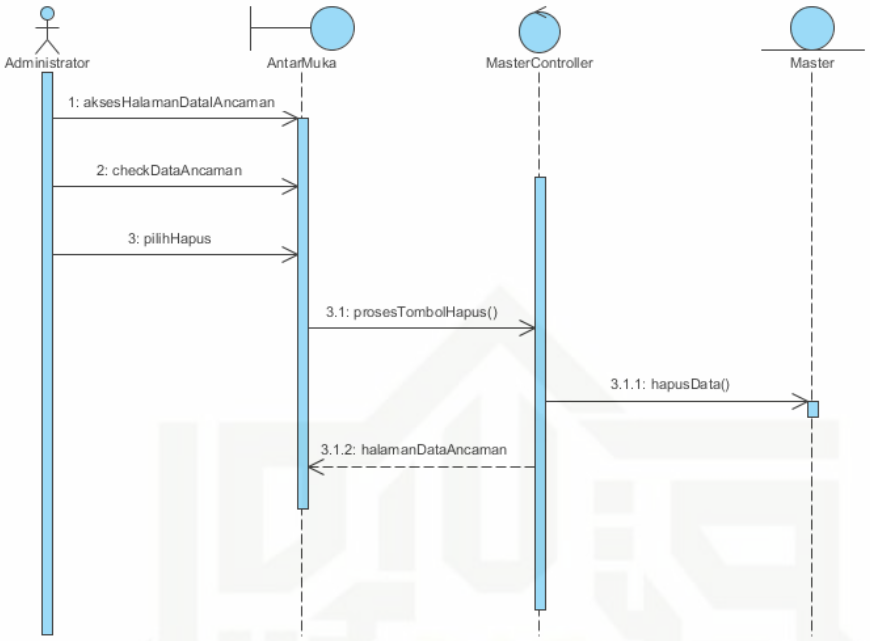
Untuk lebih jelas lagi berikut adalah *sequence diagram* ubah data ancaman pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 12 *Sequence Diagram* Ubah Data Ancaman

c. *Sequence diagram* hapus data ancaman

Proses hapus data ancaman dimulai dari saat *administrator* ingin menghapus data ancaman. Pertama *administrator* mengakses halaman data ancaman kemudian *check* pada data ancaman yang akan dihapus lalu *administrator* menekan tombol hapus, setelah itu *controller* memproses proses hapu dan menampilkan halaman data ancaman. Lebih jelas lagi berikut adalah *sequence diagram* hapus data ancaman pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



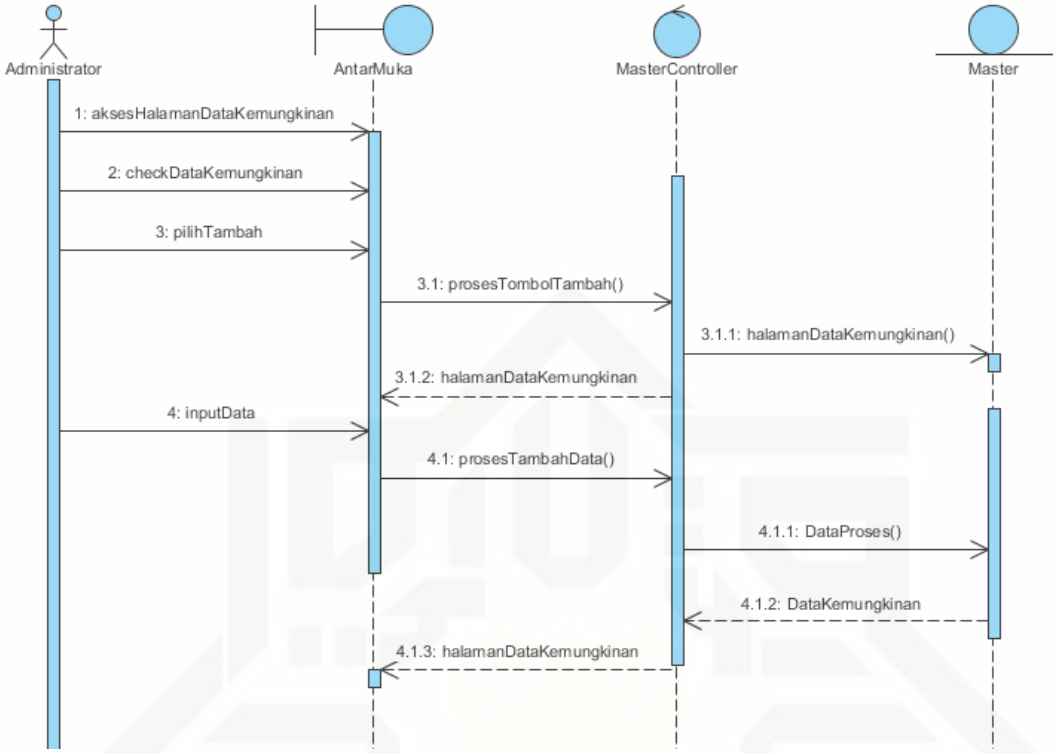
Gambar 4. 13 *Sequence Diagram* Hapus Data Ancaman

5. *Sequence Diagram* Manajemen Kemungkinan

Sequence diagram manajemen data kemungkinan berfungsi untuk menunjukan kondisi dan alur dari proses pengolahan data kemungkinan oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut adalah *Sequence diagram* dari masing-masing proses yang ada di manajemen kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

a. *Sequence diagram* tambah data kemungkinan

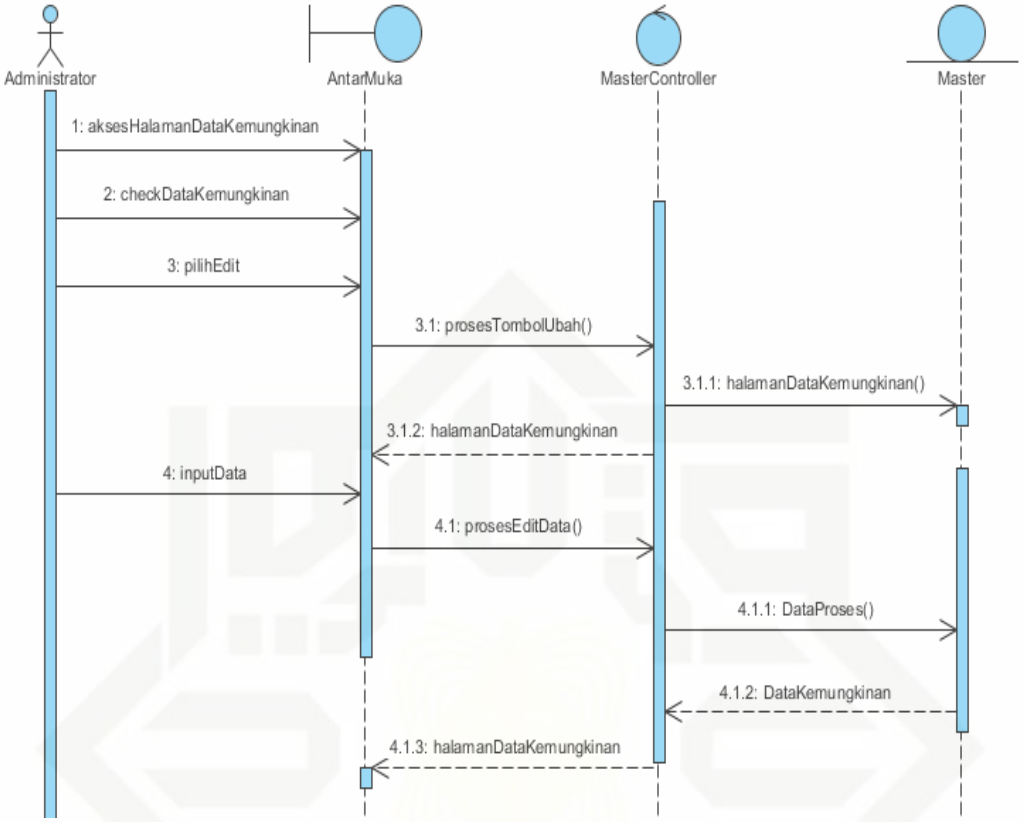
Proses tambah dimulai dari saat *administrator* ingin menambah data kemungkinan. Pertama *administrator* mengakses halaman data kemungkinan kemudian *check* pada data kemungkinan yang akan ditambah lalu *administrator* menekan tombol tambah kemungkinan, setelah itu *controller* memproses proses tambah dan menampilkan halaman tambah kemungkinan, lalu *administrator* mengisi data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* tambah data kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 14 *Sequence Diagram* Tambah Data Kemungkinan

b. *Sequence diagram* ubah data kemungkinan

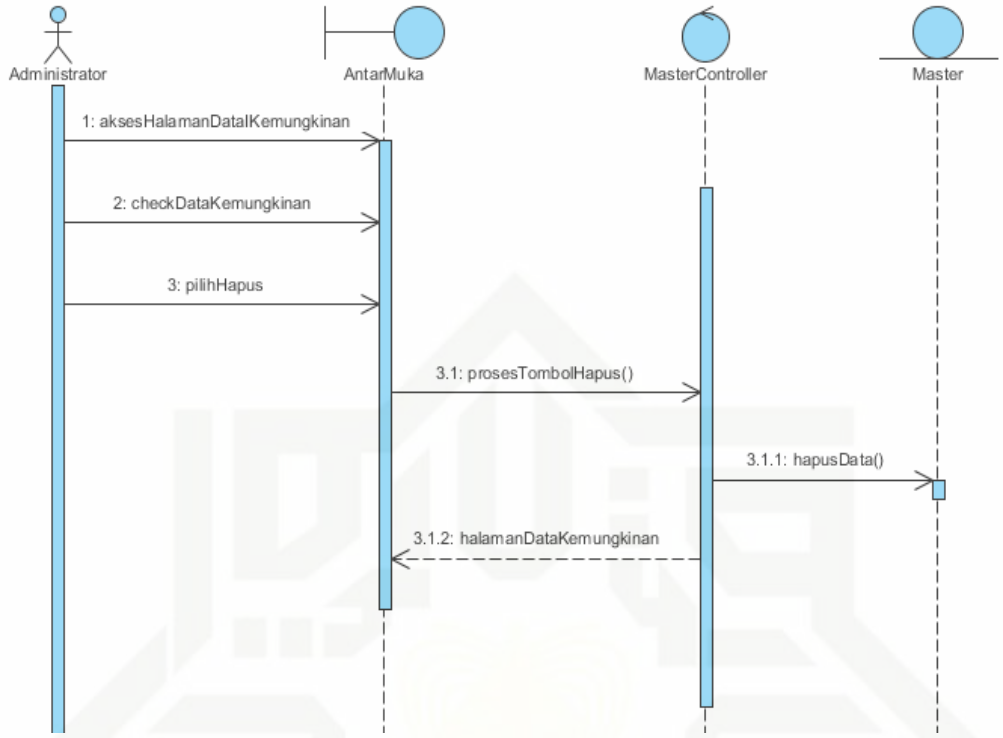
Proses ubah dimulai dari saat *administrator* ingin merubah data kemungkinan. Pertama *administrator* mengakses halaman data kemungkinan kemudian *check* pada data kemungkinan yang akan dirubah lalu *administrator* menekan tombol *edit*, setelah itu *controller* memproses proses edit dan menampilkan halaman *edit* data kemungkinan, lalu *administrator* mengisi data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* ubah data kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 15 *Sequence Diagram* Ubah Data Kemungkinan

c. *Sequence diagram* hapus data kemungkinan

Proses hapus data kemungkinan dimulai dari saat *administrator* ingin menghapus data kemungkinan. Pertama *administrator* mengakses halaman data kemungkinan kemudian *check* pada data kemungkinan yang akan dihapus lalu *administrator* menekan tombol hapus, setelah itu *controller* memproses proses hapu dan menampilkan halaman data kemungkinan. Untuk lebih jelas lagi berikut adalah *sequence diagram* hapus data kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 16 *Sequence Diagram* Hapus Data Kemungkinan

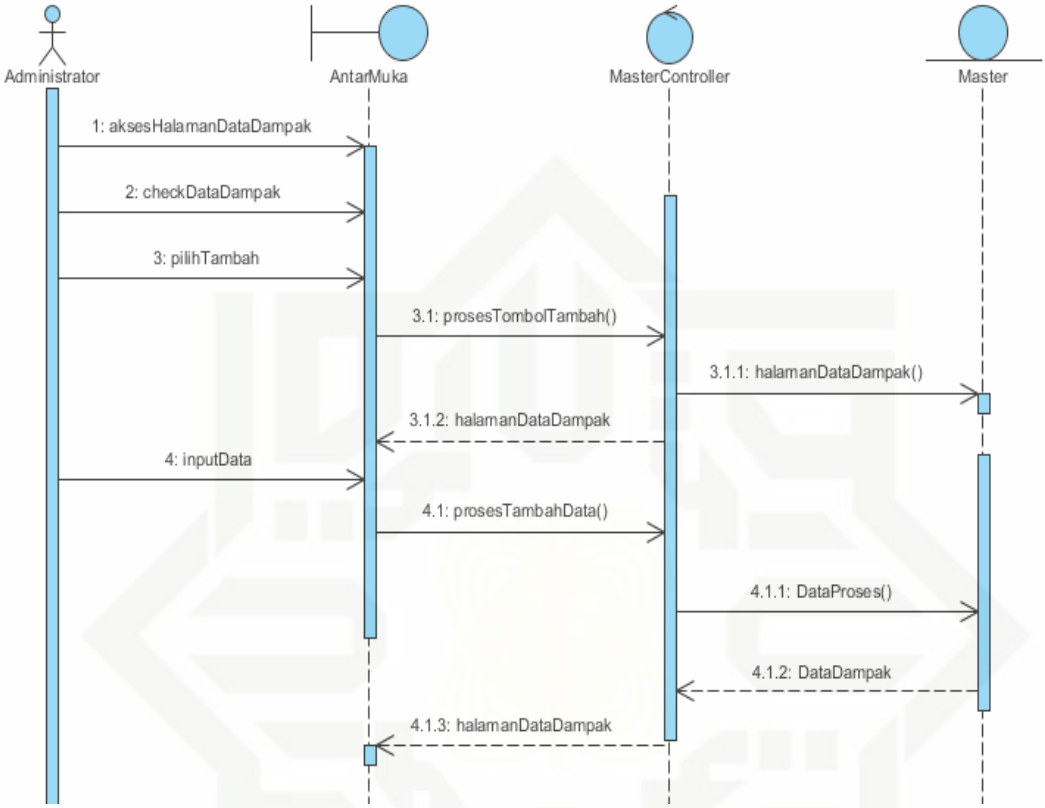
6. *Sequence Diagram* Manajemen Dampak

Sequence diagram manajemen data dampak berfungsi untuk menunjukan kondisi dan alur dari proses pengolahan data dampak oleh *administrator*, adapun proses mengolah data ialah (tambah, ubah, dan hapus). Berikut adalah *Sequence diagram* dari masing-masing proses yang ada di manajemen dampak pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

a. *Sequence diagram* tambah data dampak

Proses tambah dimulai dari saat *administrator* ingin menambah data dampak. Pertama *administrator* mengakses halaman data dampak kemudian *check* pada data dampak yang akan ditambah lalu *administrator* menekan tombol tambah dampak, setelah itu *controller* memproses proses tambah dan menampilkan halaman tambah dampak, lalu *administrator* mengisi data dan menekan tombol *submit*. Untuk lebih jelas lagi berikut adalah *sequence diagram* tambah data dampak

pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:

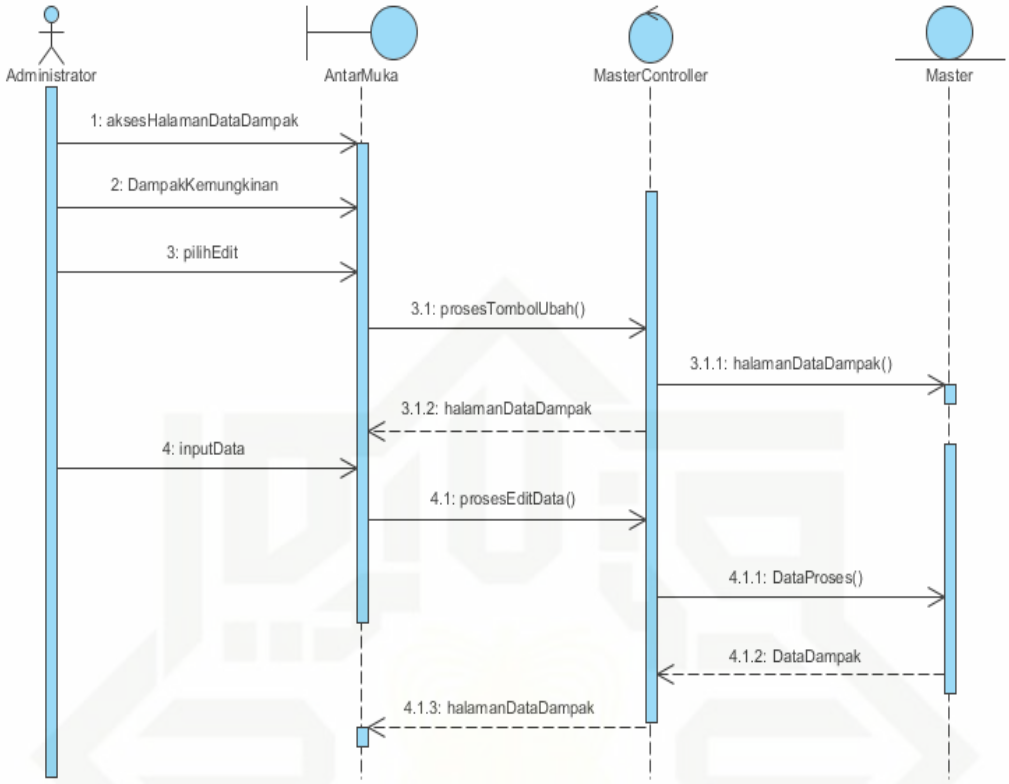


Gambar 4. 17 *Sequence Diagram* Tambah Data Dampak

b. *Sequence diagram* ubah data dampak

Proses ubah dimulai dari saat *administrator* ingin merubah data dampak. Pertama *administrator* mengakses halaman data dampak kemudian *check* pada data dampak yang akan dirubah lalu *administrator* menekan tombol *edit*, setelah itu *controller* memproses proses edit dan menampilkan halaman *edit* data dampak, lalu *administrator* mengisi data dan menekan tombol *submit*.

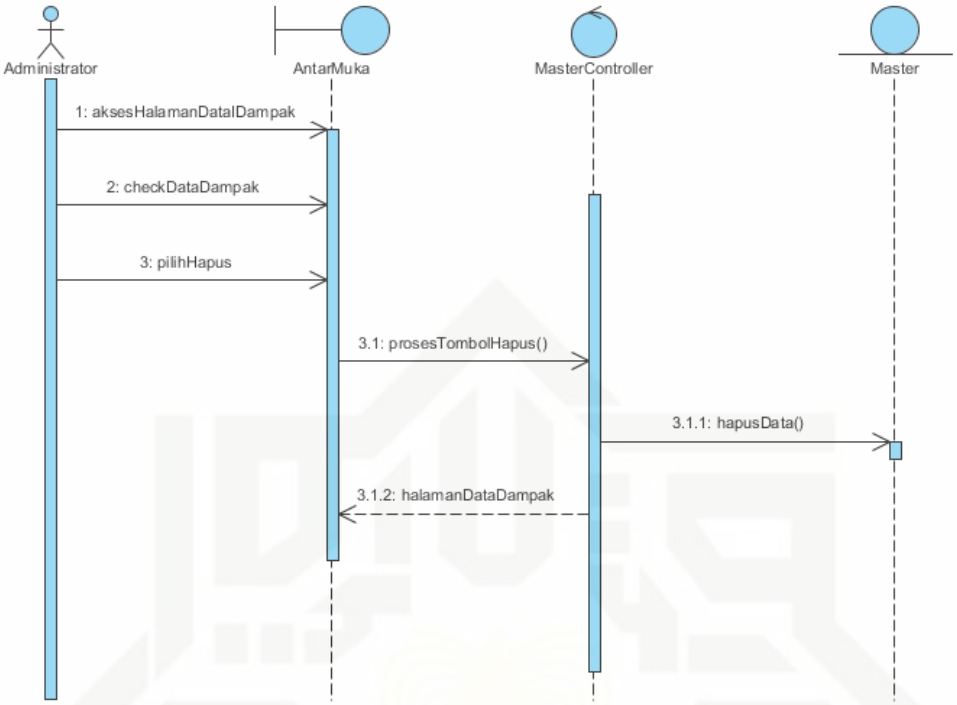
Untuk lebih jelas lagi berikut adalah *sequence diagram* ubah data dampak pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 18 *Sequence Diagram* Ubah Data Dampak

c. *Sequence diagram* hapus data dampak

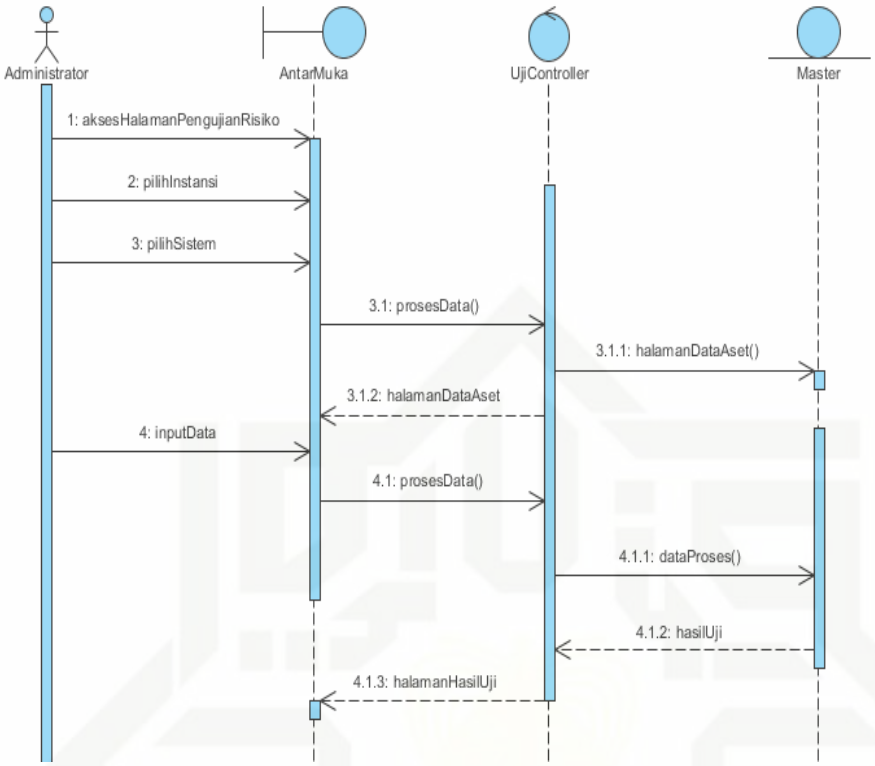
Proses hapus data dampak dimulai dari saat *administrator* ingin menghapus data dampak. Pertama *administrator* mengakses halaman data dampak kemudian *check* pada data dampak yang akan dihapus lalu *administrator* menekan tombol hapus, setelah itu *controller* memproses proses hapu dan menampilkan halaman data dampak. Untuk lebih jelas lagi berikut adalah *sequence diagram* hapus data dampak pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 19 *Sequence Diagram* Hapus Data Dampak

7. ***Sequence Diagram*** **Pengujian Risiko**

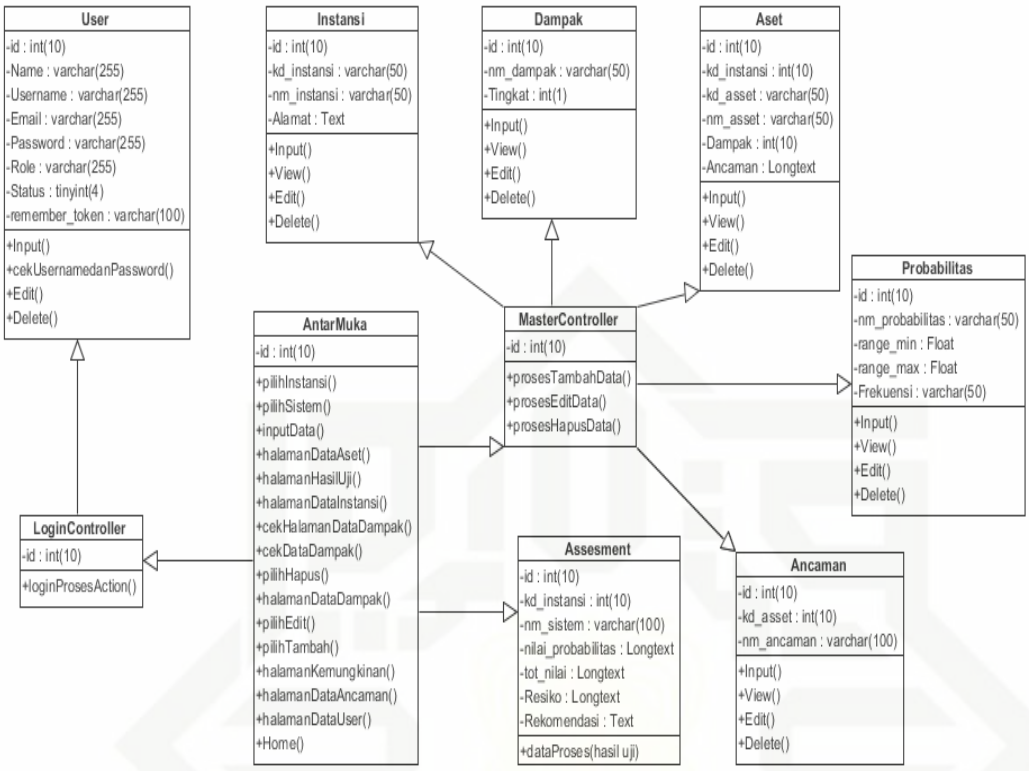
Proses ini dimulai ketika *administrator* ingin menguji atau menilai risiko dengan menggunakan Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. *Administrator* membuka halaman pengujian risiko, lalu *administrator* dihadapkan dengan pilihan instansi. Kemudian *administrator* mengisi nilai ancaman pada setiap aset sistem informasi, lalu *administrator* juga memilih dampak untuk setiap aset pada sistem informasi. Setelah itu *administrator* menekan tombol uji, lalu *controller* memproses data dan menampilkan hasil dari penilaian risiko yang berupa tingkat risiko pada setiap aset sistem informasi yang diuji tersebut. Untuk lebih jelas lagi berikut adalah *sequence diagram* pengujian risiko pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 20 *Sequence Diagram* Pengujian Risiko

E. *Class Diagram*

Class adalah sebuah spesifikasi yang jika diinstansiasi akan menghasilkan sebuah objek dan merupakan inti dari pengembangan dan desain berorientasi objek. *Class* menggambarkan keadaan (atribut/properti) suatu sistem, sekaligus menawarkan layanan untuk memanipulasi keadaan tersebut (metoda/fungsi). Kelas-kelas yang ada pada struktur sistem harus dapat melakukan fungsi-fungsi sesuai dengan kebutuhan sistem. Kelas pengguna adalah kelas yang merupakan tabel yang bisa di akses untuk segala proses yang berhubungan dengan data pengguna. Kelas *Login Controller* merupakan kelas yang menghubungkan antara antar muka login dan model pengguna. Berikut ini adalah *class diagram* dari sistem penilaian risiko keamanan informasi menggunakan metode NIST Sp 800-30 pada sistem akademik di UIN Suska Riau:

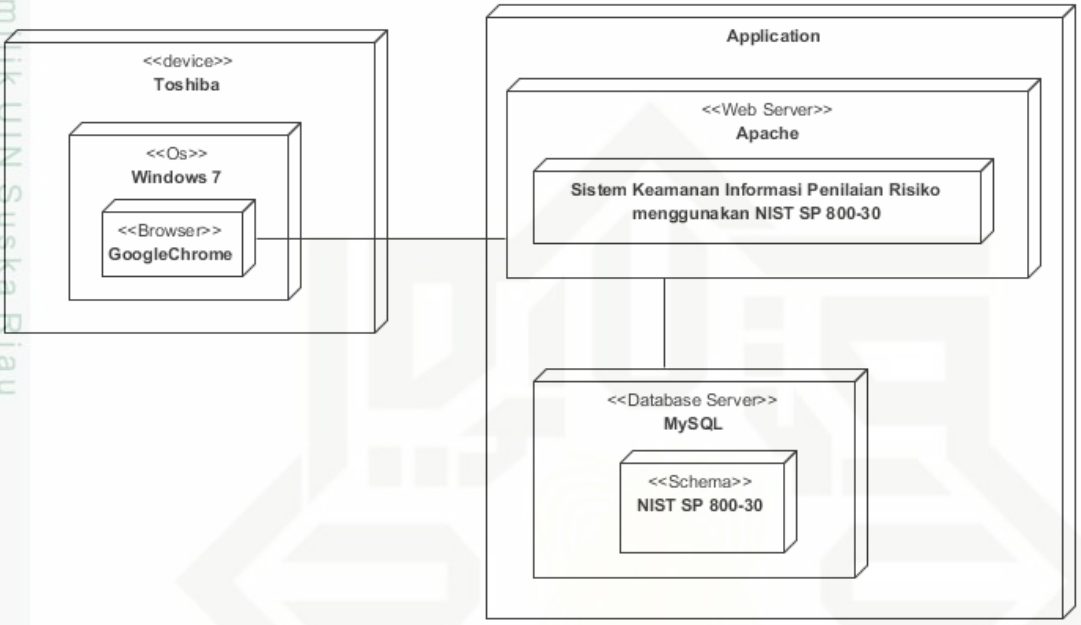


Gambar 4. 21 *Class Diagram*

F. *Deployment Diagram*

Deployment diagram merupakan gambaran proses-proses berbeda pada suatu sistem yang berjalan dan bagaimana relasi di dalamnya. Hal inilah yang mempermudah user dalam pemakaian sistem yang telah dibuat dan diagram tersebut merupakan diagram yang statis. Misalnya untuk mendeskripsikan sebuah situs web, deployment diagram menunjukkan komponen perangkat keras ("*node*") apa yang digunakan (misalnya, *web server*, server aplikasi, dan *database server*), komponen perangkat lunak ("artefak") apa yang berjalan pada setiap node (misalnya, *aplikasi web*, *database*), dan bagaimana bagian-bagian yang berbeda terhubung (misalnya JDBC, REST, RMI). *Node* digambarkan sebagai kotak, dan artefak yang dialokasikan ke setiap node digambarkan sebagai persegi panjang di dalam kotak. *Node* mungkin memiliki *subnodes*, yang digambarkan sebagai kotak *nested*. Sebuah *node* tunggal secara konseptual dapat mewakili banyak *node* fisik, seperti sekelompok *database server*.

Untuk lebih jelas lagi dapat dilihat pada Gambar 4.19, berikut ini adalah *deployment diagram* dari Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30:



Gambar 4. 22 *Deployment Diagram*

G. *Database*

Berikut adalah analisa struktur *database* dari Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30 yang dapat dilihat pada tabel dibawah ini.

1. Struktur tabel *user*

Tabel *user* memiliki sepuluh atribut yaitu, id, *email*, *name*, *username*, *password*, *role*, *status*, *remember_token*, *created_at*, dan *updated_at*.

Tabel 4.30 Struktur Tabel *User*

Nama	Jenis	Kosong	Bawaan
Id	int(10)	Tidak	Tidak ada
Name	varchar(255)	Tidak	Tidak ada
Username	varchar(255)	Tidak	Tidak ada
Email	varchar(255)	Ya	*NULL*
Password	varchar(255)	Ya	*NULL*
Role	varchar(255)	Tidak	*NULL*
Status	tinyint(4)	Tidak	*NULL*

Nama	Jenis	Kosong	Bawaan
remember_token	varchar(100)	Ya	*NULL*
created_at	*Timestamp*	Ya	*NULL*
updated_at	*Timestamp*	Ya	*NULL*

2. Struktur tabel instansi

Tabel instansi memiliki tujuh atribut yaitu, id, kd_instansi, nm_instansi, alamat, *created_at*, *updated_at*, isd. Berikut ini adalah perancangan tabel instansi:

Tabel 4.31 Struktur Tabel Instansi

Nama	Jenis	Kosong	Bawaan
Id	int(10)	Tidak	Tidak ada
kd_instansi	varchar(50)	Tidak	Tidak ada
nm_instansi	varchar(50)	Tidak	Tidak ada
Alamat	*Text*	Ya	*NULL*
created_at	*Datetime*	Ya	*NULL*
updated_at	*Timestamp*	Ya	*NULL*
Isd	Int(1)	Ya	*NULL*

3. Struktur tabel aset

Tabel aset memiliki tujuh atribut yaitu, id, kd_instansi, nm_instansi, alamat, *created_at*, danlainya. Berikut ini adalah perancangan tabel aset:

Tabel 4. 32 Struktur Tabel Aset

Kolom	Jenis	Tak Ternilai	Bawaan
Id	int(10)	Tidak	*Auto Increment*
kd_instansi	int(10)	Ya	*NUUL*
kd_*asset*	varchar(50)	Ya	*NUUL*
nm_*asset*	varchar(50)	Ya	*NUUL*
Dampak	int(10)	Ya	*NUUL*
Ancaman	*Longtext*	Tidak	Tidak ada
created_at	*Timestamp*	Ya	*NUUL*
updated_at	*Datetime*	Ya	*NUUL*
Isd	enum('1', '0')	Ya	*NUUL*

4. Struktur tabel ancaman

Tabel ancaman memiliki enam atribut yaitu, id, kd_*asset*, nm_ancaman, *created_at*, *updated_at*, dan isd. Berikut ini adalah perancangan *tabel* ancaman:

Tabel 4. 33 Struktur Tabel Ancaman

Nama	Jenis	Kosong	Bawaan
Id	int(10)	Tidak	Tidak ada
kd_asset	int(10)	Ya	*NULL*
nm_ancaman	varchar(100)	Ya	*NULL*
created_at	*Datetime*	Ya	*NULL*
updated_at	*Timestamp*	Tidak	Tidak ada
Isd	Int(1)	Ya	*NULL*

5. Struktur tabel probabilitas

Tabel probabilitas memiliki delapan atribut yaitu, id, nm_probabilitas, *range_min*, *range_max*, frekuensi, *created_at*, *updated_at*, dan isd. Berikut ini adalah perancangan tabel probabilitas:

Tabel 4. 34 Struktur Tabel Probabilitas

Nama	Jenis	Kosong	Bawaan
Id	int(10)	Tidak	Tidak ada
nm_probabilitas	varchar(50)	Ya	NULL
range_min	Float	Ya	NULL
range_max	Float	Ya	NULL
Frekuensi	varchar(50)	Ya	NULL
created_at	Datetime	Ya	NULL
updated_at	Timestamp	Tidak	Tidak ada
Isd	Int(1)	Ya	NULL

6. Struktur tabel dampak

Tabel dampak memiliki enam atribut yaitu, id, nm_dampak, tingkat, *created_at*, *updated_at*, dan isd. Berikut ini adalah perancangan tabel dampak:

Tabel 4. 35 Struktur Tabel Dampak

Nama	Jenis	Kosong	Bawaan
Id	int(10)	Tidak	Tidak ada
nm_dampak	varchar(50)	Ya	*NULL*
Tingkat	int(1)	Ya	*NULL*
created_at	*Datetime*	Ya	*NULL*
updated_at	*Timestamp*	Tidak	Tidak ada
Isd	Int(1)	Ya	*NULL*

7. **Struktur tabel *assessment***

Tabel probabilitas memiliki delapan atribut yaitu, id, kd_instansi, nm_sistem, nilai_probabilitas, tot_nilai, resiko, rekomendasi, *created_at*, *updated_at*, dan isd. Berikut ini adalah perancangan tabel probabilitas:

Tabel 4.36 Struktur Tabel *Assessment*

Nama	Jenis	Kosong	Bawaan
Id	int(10)	Tidak	Tidak ada
kd_instansi	int(10)	Ya	NULL
nm_sistem	varchar(100)	Ya	NULL
nilai_probabilitas	*Longtext*	Ya	NULL
tot_nilai	*Longtext*	Ya	NULL
Resiko	*Longtext*	Ya	NULL
Rekomendasi	*Text*	Ya	NULL
created_at	Datetime	Ya	NULL
updated_at	Timestamp	Tidak	Tidak ada
Isd	Int(1)	Ya	NULL

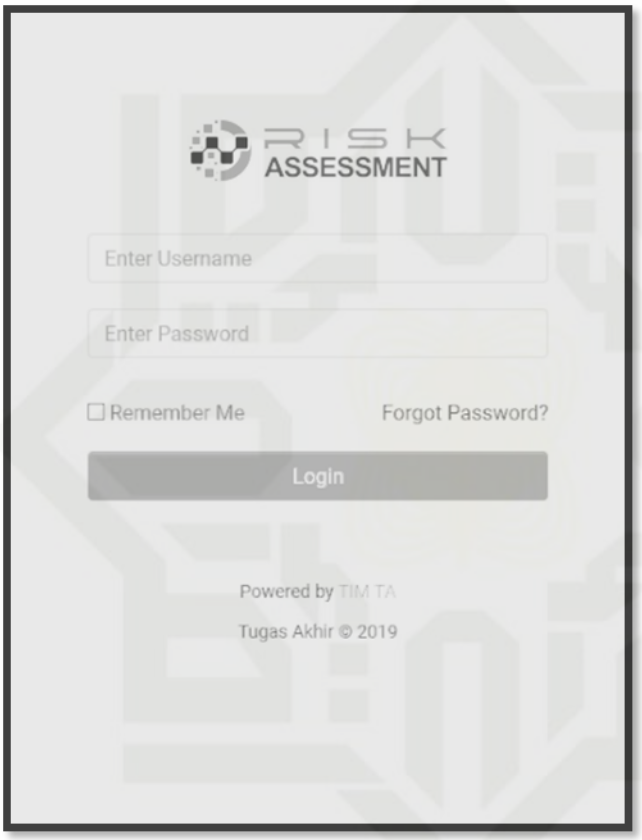
H. Perancangan Antarmuka

Antarmuka merupakan salah satu bagian yang terpenting dari sistem. Antarmuka pengguna (*user interface*) merupakan mekanisme komunikasi antara pengguna (*user*) dengan sistem. Antarmuka pemakai dapat menerima informasi dari pengguna (*user*) dan memberikan informasi kepada pengguna (*user*) untuk membantu mengarahkan alur penelusuran masalah sampai ditemukan suatu solusi. Berikut ini akan dijelaskan antarmuka yang akan digunakan dalam Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30 yang akan dirancang. Pada tahap perancangan antarmuka ini merupakan tahap perancangan *prototype* tampilan sistem yang akan dibuat, tujuan dilakukannya perancangan

interface adalah untuk memudahkan dalam proses implementasi sistem kedepannya sehingga pekerjaan menjadi lebih cepat dan efisien.

1. ***Login***

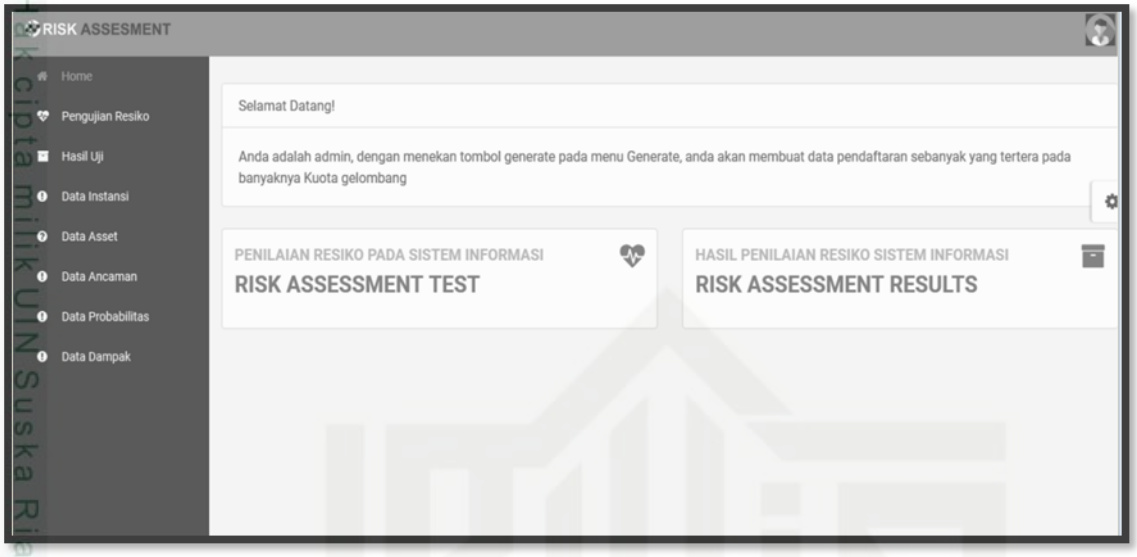
   Berikut ini adalah perancangan antarmuka halaman *login*, halaman ini digunakan bagi pengguna untuk masuk ke sistem. Untuk lebih jelas dapat dilihat pada Gambar 4.22:



Gambar 4. 23 Halaman Login

2. **Halaman Menu *Home***

Berikut ini adalah halaman menu *home*, halaman ini adalah halaman pertama yang ditampalkan oleh sistem saat pertama kali *administrator* memasuki Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.23:



Gambar 4. 24 Halaman Menu *Home*

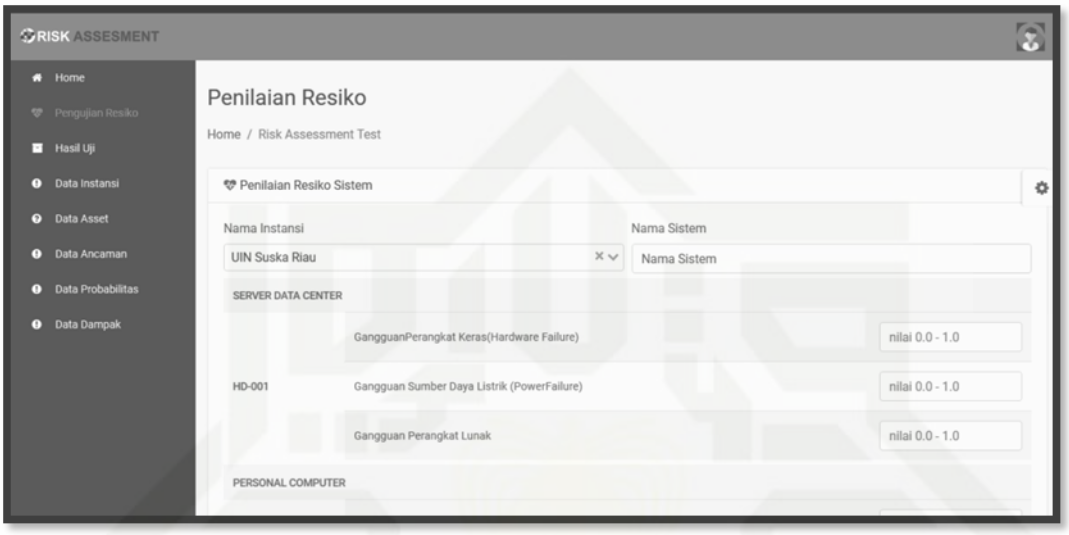
3. Halaman Awal Penilaian Risiko

Berikut ini adalah halaman awal penilaian risiko pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.24:

Gambar 4. 25 Halaman Awal Penilaian Risiko

4. Halaman Penilain Risiko

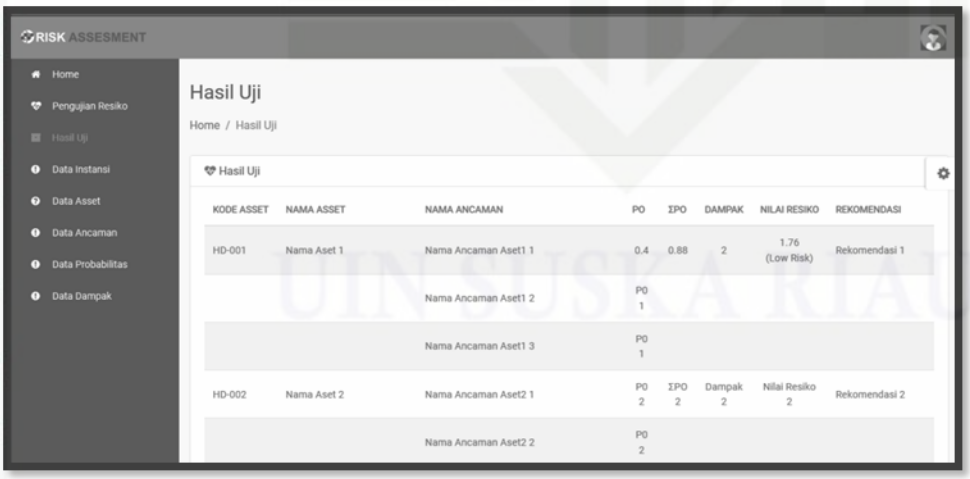
Berikut ini adalah halaman penilaian risiko pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.25:



Gambar 4. 26 Halaman Penilaian Risiko

5. Halaman Hasil Uji

Berikut ini adalah halaman hasil uji, halaman ini adalah halaman yang digunakan untuk melakukakan pengujian risiko . Untuk lebih jelas dapat dilihat pada Gambar 4.26:



Gambar 4. 27 Halaman Hasil Uji

6. Halaman Data Instansi

Berikut ini adalah halaman data instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.27:

Gambar 4. 28 Halaman Data Instansi

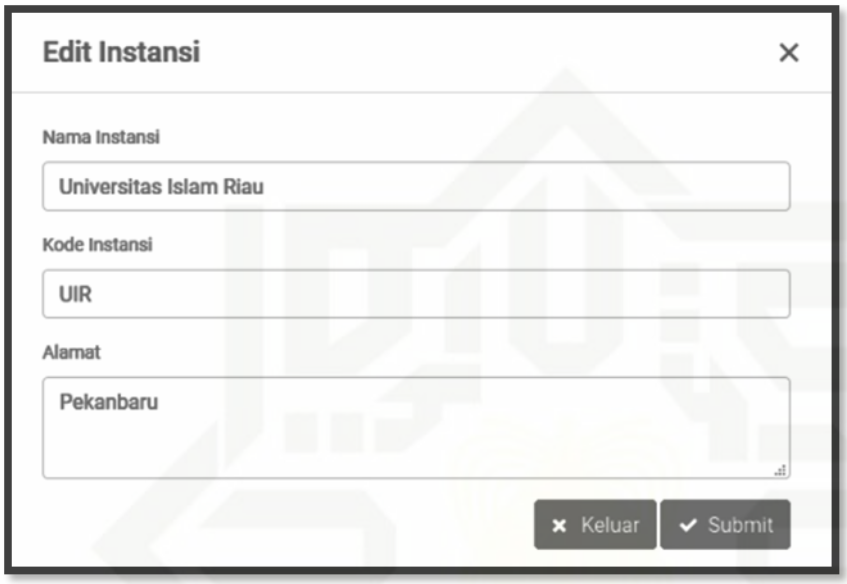
7. Halaman Tambah Data Instansi

Berikut ini adalah halaman tambah data instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.28:

Gambar 4. 29 Halaman Tambah Data Instansi

8. Halaman Ubah Data Instansi

Berikut ini adalah halaman ubah data instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.29:



Gambar 4. 30 Halaman Ubah Data Instansi

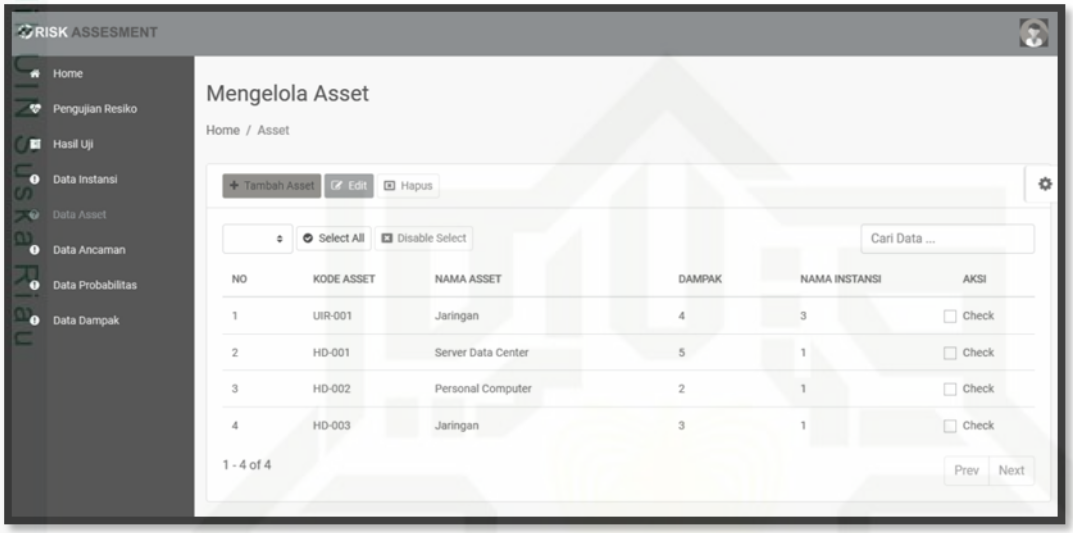
9. Halaman Hapus Data Instansi

Berikut ini adalah halaman ubah data instansi pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.30:

Gambar 4. 31 Halaman Hapus Data Instansi

10. Halaman Data Aset

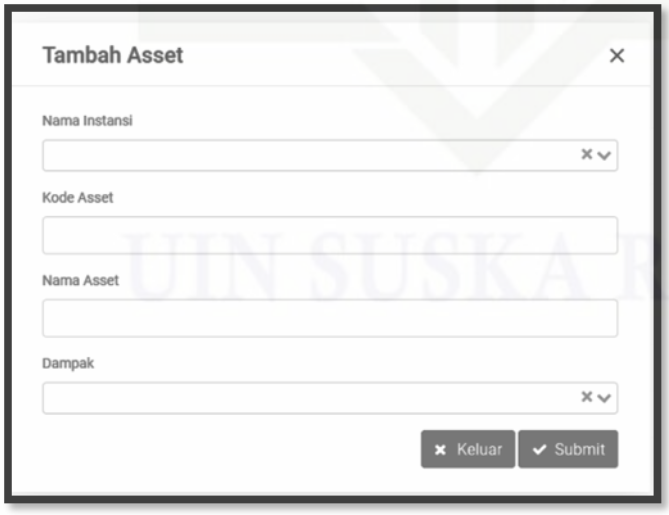
Berikut ini adalah halaman data aset pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.31:



Gambar 4. 32 Halaman Data Aset

11. Halaman Tambah Data Aset

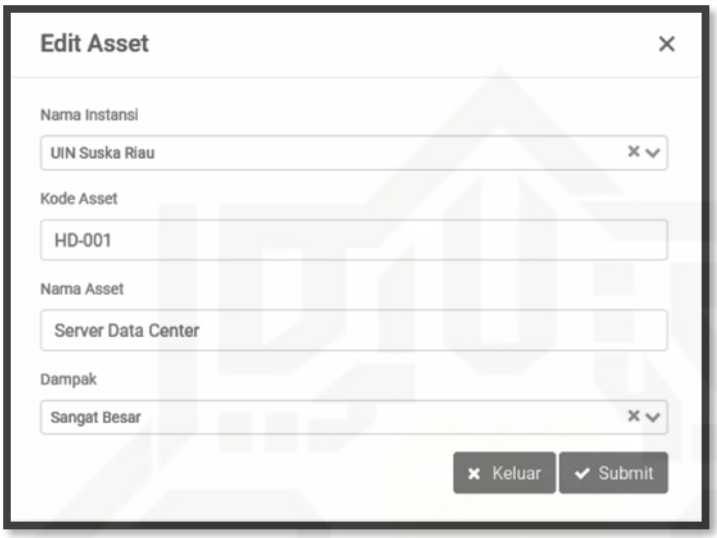
Berikut ini adalah halaman tambah data aset pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.32:



Gambar 4. 33 Halaman Tambah Data Aset

12. Halaman Ubah Data Aset

Berikut ini adalah halaman awal penilaian risiko pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.33:



Gambar 4. 34 Halaman Ubah Data Aset

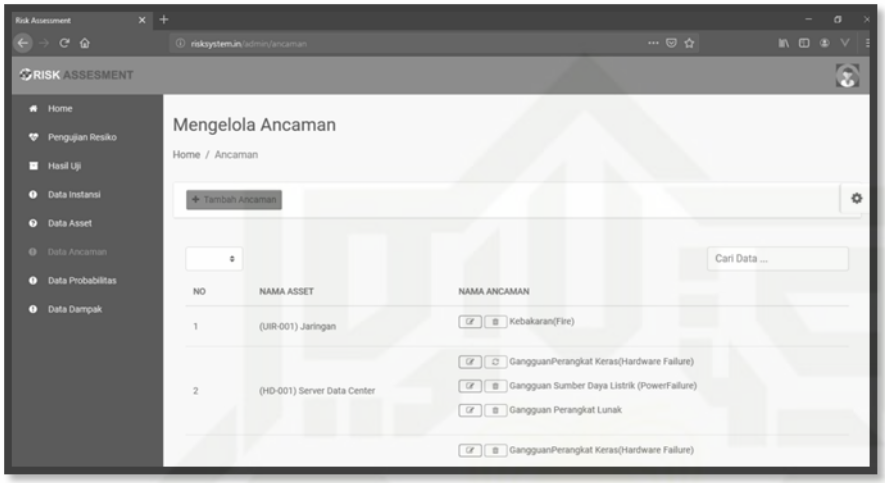
13. Halaman Hapus Data Aset

Berikut ini adalah halaman awal penilaian risiko pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.34:

Gambar 4. 35 Halaman Hapus Data Aset

14. Halaman Data Ancaman

Berikut ini adalah halaman data ancaman pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.35:



Gambar 4. 36 Halaman Data Ancaman

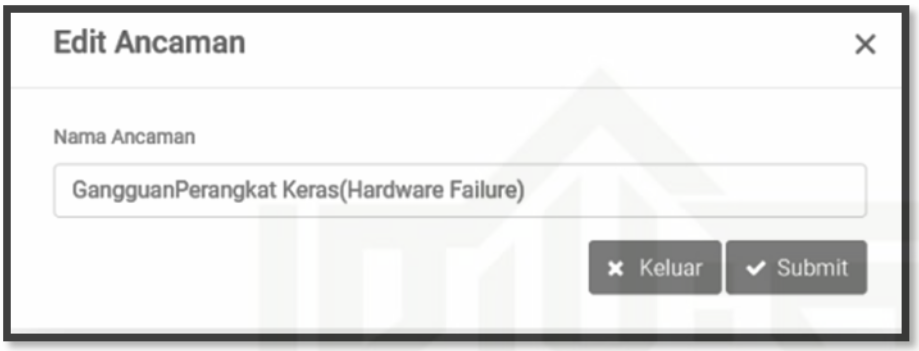
15. Halaman Tambah Data Ancaman

Berikut ini adalah halaman tambah data ancaman pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.36:

Gambar 4. 37 Halaman Tambah Data Ancaman

16. Halaman Ubah Data Ancaman

Berikut ini adalah halaman ubah data ancaman pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.37:



Gambar 4. 38 Halaman Ubah Data Ancaman

17. Halaman Hapus Data Ancaman

Berikut ini adalah halaman awal penilaian risiko pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.38:

Gambar 4. 39 Halaman Hapus Data Ancaman

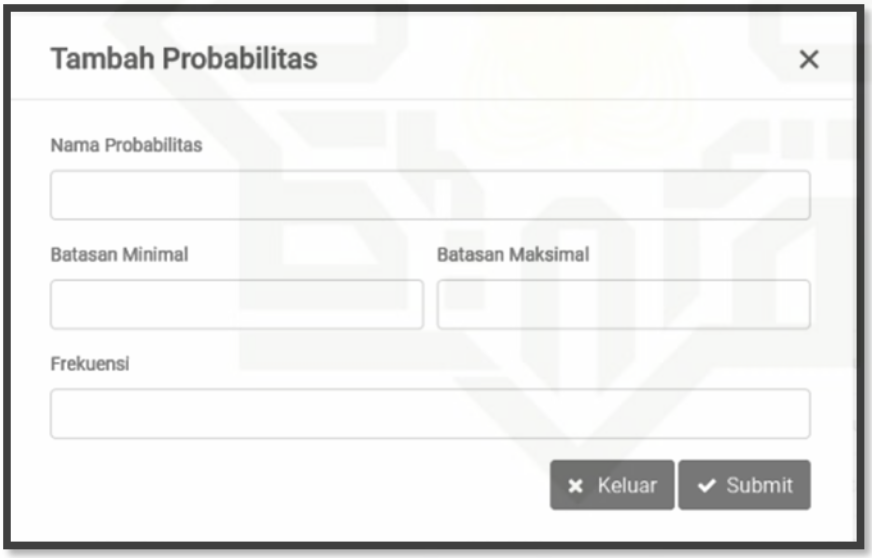
18. Halaman Data Kemungkinan

Berikut ini adalah halaman awal Data Kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.39:

Gambar 4. 40 Halaman Data Kemungkinan

19. Halaman Tambah Data Kemungkinan

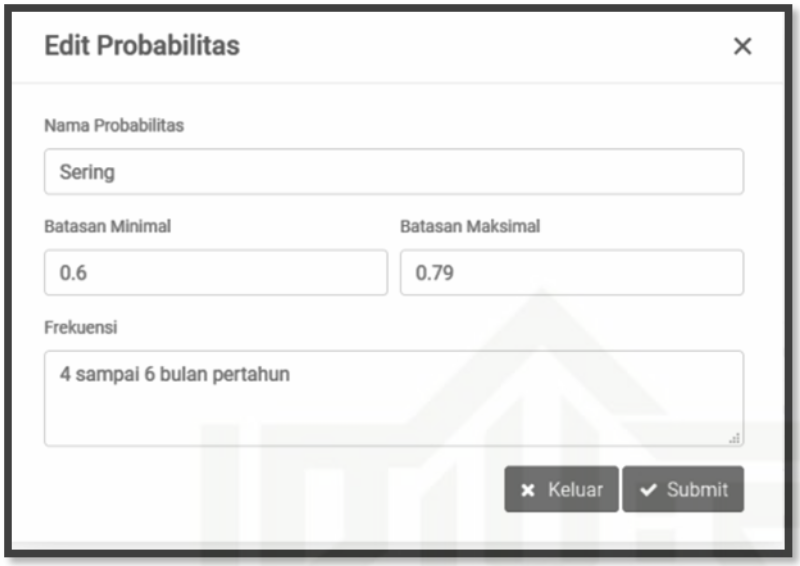
Berikut ini adalah halaman tambah data kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.40:



Gambar 4. 41 Halaman Tambah Data Kemungkinan

20. Halaman Ubah Data Kemungkinan

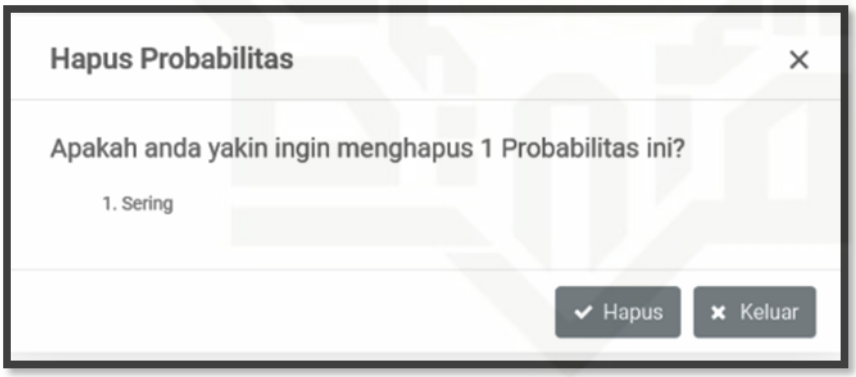
Berikut ini adalah halaman ubah data kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.41:



Gambar 4. 42 Halaman Ubah Data Kemungkinan

21. Halaman Hapus Data Kemungkinan

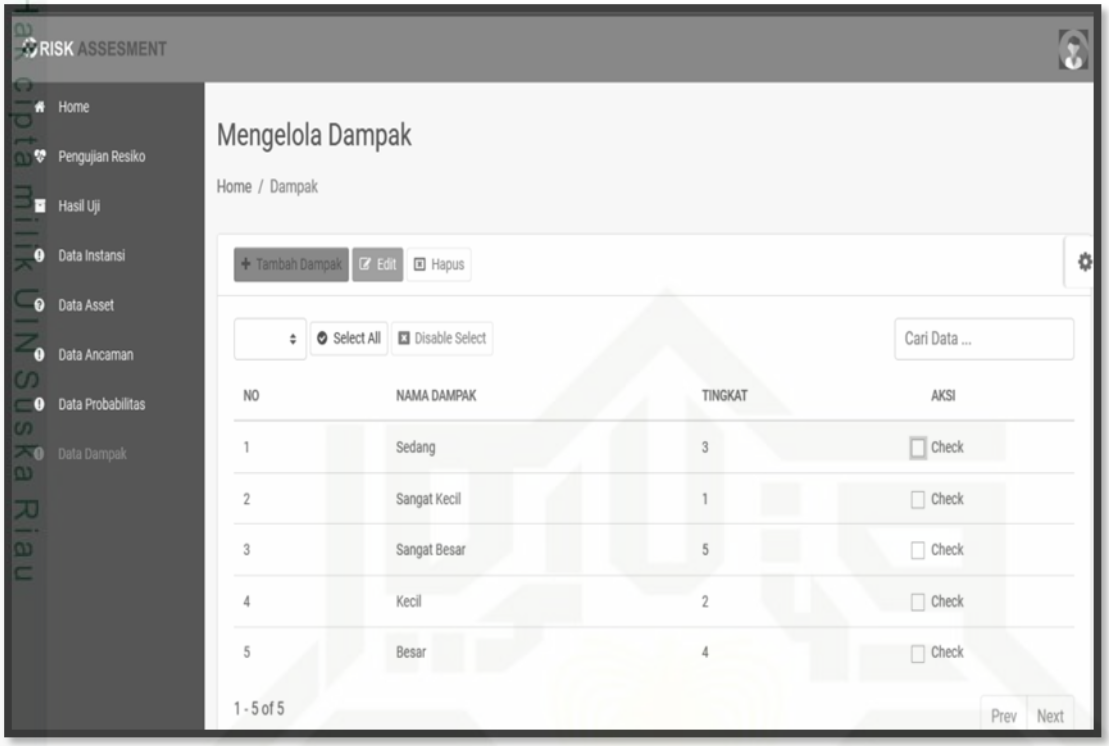
Berikut ini adalah halaman hapus data kemungkinan pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.42:



Gambar 4. 43 Halaman Hapus Data Kemungkinan

22. Halaman Data Dampak

Berikut ini adalah halaman awal halaman dampak pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.43:



Gambar 4. 44 Halaman Data Dampak

23. Halaman Tambah Data Dampak

Berikut ini adalah halaman tambah data dampak pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.44:

Gambar 4. 45 Halaman Tambah Data Dampak

24. Halaman Ubah Data Dampak

Berikut ini adalah halaman ubah data dampak pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.45:

Gambar 4. 46 Halaman Ubah Data Dampak

25. Halaman Hapus Data Dampak

Berikut ini adalah halaman hapus data dampak pada Sistem Penilaian Risiko Keamanan Informasi menggunakan NIST SP 800-30. Untuk lebih jelas dapat dilihat pada Gambar 4.46:

Gambar 4. 47 Halaman Hapus Data Dampak

BAB VI
PENUTUP

6.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan terkait dengan pelaksanaan penilaian risiko keamanan informasi pada aset yang mendukung Sistem Akademik UIN Suska Riau, maka penulis dapat memberikan suatu kesimpulan penelitian sebagai berikut:

1. Pada Penelitian ini diterapkan Metode NIST SP 800-30 terhadap Sistem Akademik UIN Suska Riau yang memiliki *output* Sistem Penilaian Risiko Keamanan Informasi.
2. Hasil dari penilaian menggunakan Sistem Penilaian Risiko Keamanan Informasi menggunakan Metode NIST SP 800-30 terhadap Sistem Akademik UIN Suska Riau; didapatkan lima (5) risiko level sedang yaitu Komputer, UPS, Karyawan, Sistem Informasi Pendaftaran Mahasiswa Baru (PMB) dan Sistem Regristasi (Sireg), empat (4) risiko level tinggi yaitu: Iraise, Server, Jaringan dan Informasi Nilai Mahasiswa.
3. Sistem informasi yang dibangun memiliki rata-rata tingkat akurasi berdasarkan aspek penilaian pengujian UAT dengan kategori: informatif sebesar 82,66%, kemudahan penggunaan 80,00%, ketepatan waktu sistem sebesar 83,20% dan kehandalan sistem sebesar 86,66%.

6.2 Saran

Berikut adalah saran yang diberikan oleh peneliti sebagai berikut ini:

1. Mengacu kepada hasil dari penilaian risiko pada penelitian ini, PTIPD selaku pengampu sistem akademik dapat menerapkan beberapa rekomendasi yang sudah didapatkan dari hasil penelitian ini.
2. Pada penelitian selanjutnya dapat menerapkan metode NIST dengan seri SP 800-37, SP 800-53, SP 800-171 untuk dilakukan penilaian risiko yang lebih kompleks.

DAFTAR PUSTAKA

Albana, A. S. and Saputra, A. (2012) 'Pengembangan Metode Manajemen Risiko untuk Keputusan Kelayakan Investasi yang mempertimbangkan Ketidakpastian', (July).

Alberts, C. and Dorofee, A. (2002) *Managing information security risks : the OCTAVE approach*.

gary stonebumer, alice goguen, and alexis feringa (2002) 'Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology', 30(July).

Grover, K. (2007) *Kenneth C. Laudon and Jane P. Laudon, Management Information System - Managing the Digital Firm (ninth ed.), Prentice-Hall, New Jersey (2005) ISBN: 0-131-53841-1., Inf. Process. Manage.* doi: 10.1016/j.ipm.2007.01.007.

McLeod, R. and Schell, G. (2006) *Management Information Systems (10th Edition)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc.

National Institute of Standards and Technology Gaithersburg (2012) 'Guide for conducting risk assessments', *NIST Special Publication*, (1), p. 95. doi: 10.6028/NIST.SP.800-30r1.

Nurochman, A. (2014) 'Manajemen Risiko Sistem Informasi Perpustakaan (Studi Kasus di Perpustakaan UGM Yogyakarta'.

Paryati (2008) 'Keamanan sistem informasi', 2008(semnasIF), pp. 379–386.

Permatasari, M. *et al.* (2016) 'Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799 : 2000', 02, pp. 97–104. doi: 10.21456/vol6iss2pp97-104.

Ricci, F., Rokach, L. and Shapira, B. (2011) *Recommender System Handbook*. New York: Springer.

Stoneburner, G., Gougen, A. and Feringa, A. (2002) *NIST SP 800-30 - Risk Management Guide for Information Technology Systems, Computer Security Division*. doi: 10.6028/NIST.SP.800-30r1.

Stulz, R. M. (2008) 'Risk Management Failures: What Are They and When Do They Happen?', *Journal of Applied Corporate Finance*, 20(4), pp. 39–48. doi: 10.1111/j.1745-6622.2008.00202.x.

Susilo (2017) 'Analisa Tingkat Resiko Tata Kelola Teknologi Informasi Perguruan Tinggi Menggunakan Model Framework National Institute of Standards & Technology (NIST) Special Publication 800-30 dan IT General Control Questionnaire (ITGCQ)', *Journal Industrial Servicess*, Vol. 3c

Swearingen, K. and Sinha, R. (2001) 'Beyond Algorithms : An HCI Perspective on Recommender Systems', pp(in ACM SIGIR 2001 Workshop on Recommender Systems), pp. 1–11.

Syafitri, W. (2016) 'Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus : Sistem Informasi Akademik Universitas XYZ)', *CoreIT*, 2(2), pp. 8–13.

LAMPIRAN A
SURAT IZIN PENELITIAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PUSAT TEKNOLOGI INFORMASI DAN PANGKALAN DATA
مركزتكنولوخيا المعلومات وقواعد البيانات
CENTER OF INFORMATION TECHNOLOGY AND DATABASES
Jl. HR. Soebrantas No. 155 KM. 18 Simpang Baru Panam Pekanbaru 28293 PO BOX 1004 HP 0811 7627 773
Website : www.pitpd.uin-suska.ac.id Email : pitpd@uin-suska.ac.id

SURAT KETERANGAN DITERIMA TUGAS AKHIR
Nomor : Un. 04/UPT.II/PP.00.9/35/2019

Yang bertanda tangan di bawah ini menerangkan :

Nama : Melati Sukma Dewi
Nim : 11451201860
Jurusan : Teknik Informatika
Semester : X (Sepuluh)

diterima untuk melaksanakan Kerja Praktek di :

Perusahaan/Instansi : Pusat Teknologi Informasi dan Pangkalan Data UIN Suska Riau
Alamat : Jl. HR. Soebrantas No. 155 KM. 18 Simpang Baru Panam Pekanbaru
Bidang Kajian/Judul : Sistem Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST SP 800-30

Pekanbaru, 15 Februari 2019
Kepala PITPD UIN Suska Riau

Benny Sukma Negara, MT
NIP. 19820313 200901 1 009

LAMPIRAN B
WAWANCARA

WAWANCARA

Tanggal : Januari 2019
Waktu : Jum'at /22 Februari 2019
Narasumber : Riyen Perdana
Jabatan : Staf divisi Aplikasi PTIPD

Daftar pertanyaan :

1. Apa-apa saja ancaman yang pernah terjadi di Sistem Akademik UIN SUSKA RIAU?

   Jawaban:

   Ancaman yang pernah terjadi :

   a. Ikeise

      Kesalahan pembuatan Role User yang mengizinkan Role level mahasiswa menyakses Role level dosen.

   b. Sifes

      Tidak ada ancaman

   c. PMB

      Tidak ada Ancaman

2. Berapa kemungkinan terjadinya ancaman-ancaman tersebut pada Sistem Akademik UIN SUSKA RIAU?

Jawaban:

Tingkat	Sebutan	Uraian	Frekuensi
1	Sangat jarang	Hampir tidak pernah terjadi	>2 tahun
2	Jarang	Mungkin terjadi tapi jarang	1 - 2 tahun
3	Mungkin	Mungkin saja terjadi tapi jarang-jarang	7 - 12 bulan / tahun
4	Mungkin sekali	Kemungkinan besar terjadi	4 – 6 bulan / tahun
5	Hampir pasti	Hampir selalu terjadi	1 – 3 bulan / tahun

1. Reise → Tingkat 3
2. Siraj → Tingkat 1
3. Andi → Tingkat 1

3. Berapa tingkatan dampak yang terjadi disebabkan ancaman-ancaman tersebut pada Sistem Akademik UIN SUSKA RIAU?

Tingkat	Sebutan	Uraian
1	**Sangat kecil**	Dampak kecil yang dapat diabaikan
2	**Kecil**	Kerusakan kecil yang mudah diperbaiki kembali
3	**Sedang**	Mempengaruhi pencapaian beberapa sasaran
4	**Besar**	Sasaran-sasaran penting tidak dapat tercapai
5	**Sangat besar**	Semua sasaran tidak dapat tercapai

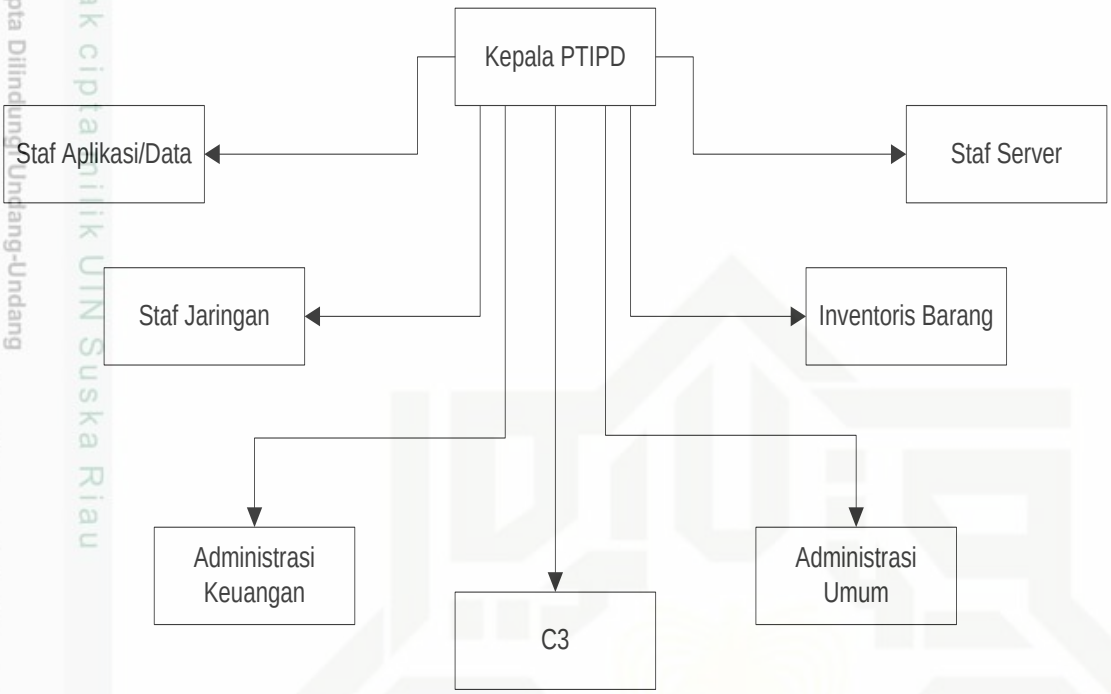
1. [illegible] → Tingkat 3
2. [illegible] → Tingkat 1
3. [illegible] → Tingkat 1

Pekanbaru, januari 2019

[illegible]

NIP. [illegible]

LAMPIRAN C
STRUKTUR ORGANISASI PUSAT TEKNOLOGI INFORMASI DAN PANGKALAN DATA UIN SUSKA RIAU



Tugas pokok bagian Pusat Teknologi Informasi dan Pangkalan Data UIN Suska Riau adalah sebagai berikut:

No	Jabatan	Tugas Pokok
1	Kepala PTIPD	1. Melakukan pengawasan terhadap aplikasi/*software* 2. Melakukan pengawasan terhadap operasional jaringan 3. Melakukan pengawasan dan pemantauan terhadap perangkat keras/*hardware* 4. Melakukan pemeliharaan dan perbaikan perangkat keras dan jaringan 5. Melakukan pemeliharaan dan perbaikan aplikasi/*software* 6. Melakukan pengembangan aplikasi Sistem
2	Bagian Aplikasi/Data	1. Melakukan analisa Sistem agar bisa di implementasikan sesuai dengan kebutuhan Akademik 2. Berkoordinasi dengan unit-unit terkait agar implementasi Akademik berjalan dengan baik 3. Melakukan sosisalisasi dan pendampingan terhadap *user* dalam penerapan kebijakan baru yang berhubungan dengan Sistem

No	Jabatan	Tugas Pokok
		Akademik 4. Mengelolah data sistem untuk kebutuhan pelaporan bagian keuangan 5. Mengakomodir permintaan dan pembuatan laporan yang dibutuhkan oleh internal melalui *query database*
2	*Custumer Care* *Center* (C3)	1. Berkoordinasi dengan atasan dalam melaksanakan tugas-tugas ketersediaan layanan 2. Membantu menyiapkan informasi dan laporan yang baik serta tepat waktu 3. Memberikan layanan *costumer service/helpdesk* 4. Membantu menyusun laporan bulanan dan tahunan pelaksanaan kegiatan 5. Membantu melaksanakan fungsi administrasi berupa pencatatan dan penyimpanan
4	Bagian Server	1. Melakukan monitoring dan evaluasi terhadap kelancaran koneksi server *2.* Melakukan pemeliharaan dan perbaikan jaringan/*hardware* 3. Membuat laporan bulanan kepada kepala PTIPD 4. Membantu melaksanakan fungsi administrasi berupa pencatatan, penyimpanan, dan pemeliharaan dokumen digital dan monitor data 5. Melakukan pencatatan kergiatan perbaikan dan pemeliharaan jaringan/*hardware* dalam *log book* baik yang bersifat rutin terjadwal atau yang bersifat insidentil
5	Bagian Jaringan	1. Melakukan monitoring dan evaluasi terhadap kelancaran jaringan sistem *2.* Melakukan pemeliharaan dan perbaikan jaringan/*hardware* 3. Membuat laporan bulanan kepada kepala PTIPD 4. Membantu melaksanakan fungsi administrasi berupa pencatatan, penyimpanan, dan pemeliharaan dokumen digital dan monitor 5. Melakukan pencatatan kergiatan perbaikan dan pemeliharaan jaringan/*hardware* dalam

No	Jabatan	Tugas Pokok
		log book baik yang bersifat rutin terjadwal atau yang bersifat insidentil
6	Administrasi Umum	1. Membantu menyiapkan informasi dan laporan yang baik serta tepat waktu untuk kebutuhan internal maupun eksternal unit kerja yang bersifat rutin 2. Membantu menyusun laporan bulanan dan tahunan pelaksanaan kegiatan PTIPD 3. Membantu melaksanakan fungsi administrasi berupa pencatatan, penyimpanan dan pemeliharaan dokumen digital dan monitor data 4. Membuat amprahan permintaan kebutuhan alat tulis kantor kepada kepala instalasi logistik 5. Melaksanakan tugas kedinasan lain yang diperintahkan oleh atasan langsung baik lisan maupun tulisan 6. Mendistribusikan surat keluar sesuai tujuan
7	Administrasi Keuangan	1. Menyusun kebijakan anggaran keuangan organisasi 2. Mengatur arus uang perusahaan 3. Membuat Rencana Keuangan Perusahaan 4. Memberikan layanan kepada *custumer* 5. Membantu menyusun laporan bulanan dan tahunan pelaksanaan kegiatan 6. Membantu melaksanakan fungsi administrasi berupa pencatatan dan penyimpanan
8	Inventaris Barang	1. Menerima, menyimpan dan menyalurkan barang milik PTIPD 2. Meneliti dan menghimpun dokumen pengadaan barang yang diterima 3. Meneliti jumlah dan kualitas barang yang diterima sesuai dengan dokumen pengadaan 4. Mencatat barang yang diterima ke dalam buku/kartu barang 5. Mengamankan barang yang ada dalam persediaan 6. Membuat laporan penerimaan, penyaluran dan persediaan barang kepada Kepala PTIPD

LAMPIRAN D
PERHITUNGAN NILAI ANCAMAN ASET

Berikut ini adalah hasil dari perhitungan nilai asset berdasarkan wawancara dengan pihak aplikasi sistem akademik.

Nilai Ancaman (NT) = Rerata Probabilitas x Total Kejadian

Tabel Perhitungan Nilai Ancaman Aset

	ID Aset: IN-001
	Jumlah Hari: 30
	Nama Aset: Informasi Nilai Mahasiswa

Kejadian		Jenis	Probabilitas	Jumlah Kejadian Per 30 hari	Rerata Probabilitas
Kode	**Keterangan**				
T1	Akses Ilegal (Unauthorized Access)	Ancaman	*Low*	2	0,0667
T3	Hackers (Intruders)	Ancaman	*Low*	1	0,0333
T6	Kebakaran (Fire)	Ancaman	*Low*	0	0
V1	Kerusakan Data (Data Corruption)	Ancaman	*Low*	0	0
V2	Kesalahan SDM (Human Error)	Ancaman	*Low*	8	0,2667
V5	Kesalahan Pengiriman Data (Data Missing Recipient)	Kelemahan	*Low*	3	0,1
V9	Tidak ada kontrol pengawasan	Kelemahan	*Low*	0	0
V10	Kurangnya tenaga ahli	Kelemahan	*Low*	0	0
Total Kejadian	8	**Jumlah Rerata Probabilitas**		14	0,4667
Nilai Ancaman (NT)					0,04243

	ID Aset: HD-001
	Jumlah Hari: 30
	Nama Aset: *Server*

Kejadian		Jenis	Probabilitas	Jumlah Kejadian Per 30 hari	Rerata Probabilitas
Kode	**Keterangan**				
T1	Akses Ilegal (Unauthorized Access)	Ancaman	*Low*	0	0
T4	Pencurian Asset (Theft of Asset)	Ancaman	*Low*	0	0
T6	Kebakaran (Fire)	Ancaman	*Low*	0	0

V2	Kesalahan SDM (Human Error)	Kelemahan	*Low*	0	0
V3	Gangguan Perangkat Keras	Kelemahan	*Low*	11	0,3666
V4	Gangguan Sumber Daya Listrik (Power Failure)	Kelemahan	*Low*	4	0,1333
V8	Tidak ada kontrol pengawasan	Kelemahan	*Low*	1	0,0333
V9	Respon pihak eksternal pada layanan	Kelemahan	*Low*	0	0
V10	Kurangnya tenaga ahli	Kelemahan	*Low*		0
Total Kejadian	9	**Jumlah Rerata Probabilitas**		15	0,5332
Nilai Ancaman (NT)					0,00593

	ID Aset: HD-002				
	Jumlah Hari: 30				
	Nama Aset: Komputer				
Kejadian		**Jenis**	**Probabilitas**	**Jumlah Kejadian Per 30 hari**	**Rerata Probabilitas**
Kode	**Keterangan**				
T1	Akses Ilegal (Unauthorized Access)	Ancaman	*Low*	0	0
T4	Pencurian Asset (Theft of Asset)	Ancaman	*Low*	3	0,1
T6	Kebakaran (Fire)	Ancaman	*Low*	0	0
V2	Kesalahan SDM (Human Error)	Kelemahan	*Low*	0	0
V3	Gangguan Perangkat Keras (Hardware Failure)	Kelemahan	*Low*	24	0,8
V4	Gangguan Sumber Daya Listrik (Power Failure)	Kelemahan	*Low*	0	0
V6	Kesalahan Fungsional Perangkat Lunak (Software Bug)	Kelemahan	*Low*	4	0,1333
V7	Pembaharuan Aplikasi	Kelemahan	*Low*	4	0,133
V8	Tidak ada kontrol pengawasan	Kelemahan	*Low*	0	0
V9	Respon pihak eksternal pada layanan	Kelemahan	*Low*	0	0
Total Kejadian	10	**Jumlah Rerata Probabilitas**		31	0,8366
Nilai Ancaman (NT)					0,06972

	ID Aset: HD-003
	Jumlah Hari: 30
	Nama Aset: Jaringan

Kejadian		Jenis	Probabilitas	Jumlah Kejadian Per 30 hari	Rerata Probabilitas
Kode	**Keterangan**				
T1	Akses Ilegal (Unauthorized Access)	Ancaman	*Low*	0	0
T6	Kebakaran (Fire)	Ancaman	*Low*	0	0
T7	Gangguan Petir (Lightining)	Ancaman	*Low*	0	0
V2	Kesalahan SDM (Human Error)	Kelemahan	*Low*	8	0,2667
V3	Gangguan Perangkat Keras (Hardware Failure)	Kelemahan	*Low*	8	0,2667
V4	Gangguan Sumber Daya Listrik (Power Failure)	Kelemahan	*Low*	8	0,2667
V8	Tidak ada kontrol pengawasan	Kelemahan	*Low*	0	0
V9	Respon pihak eksternal pada layanan	Kelemahan	*Low*	1	0,0333
V10	Kurangnya tenaga ahli	Kelemahan	*Low*	0	0
Total Kejadian	9	**Jumlah Rerata Probabilitas**		25	0,8334
Nilai Ancaman (NT)					0,0925

	ID Aset: HD-004
	Jumlah Hari: 30
	Nama Aset: UPS

Kejadian		Jenis	Probabilitas	Jumlah Kejadian Per 30 hari	Rerata Probabilitas
Kode	**Keterangan**				
T1	Akses Ilegal (Unauthorized Access)	Ancaman	*Low*	0	0
T4	Pencurian Asset (Theft of Asset)	Ancaman	*Low*	0	0
T6	Kebakaran (Fire)	Ancaman	*Low*	0	0
V2	Kesalahan SDM (Human Error)	Kelemahan	*Low*	0	0
V3	Gangguan Perangkat Keras (Hardware Failure)	Kelemahan	*Low*	1	0,0027

V4	Gangguan Sumber Daya Listrik (Power Failure)	Kelemahan	*Low*	0	0
V8	Tidak ada kontrol pengawasan	Kelemahan	*Low*	0	0
V9	Respon pihak eksternal pada layanan	Kelemahan	*Low*	0	0
V10	Kurangnya tenaga ahli	Kelemahan	*Low*	0	0
Total Kejadian	9	**Jumlah Rerata Probabilitas**		1	0,0027
Nilai Ancaman (NT)					0,0003

	ID Aset: SW-001				
	Jumlah Hari: 30				
	Nama Aset: IRaise				
Kejadian		**Jenis**	**Probabilitas**	**Jumlah Kejadian Per 30 hari**	**Rerata Probabilitas**
Kode	**Keterangan**				
T2	Serangan Virus (Virus Attack, Ex: Malware, Ransomware, Trojan, etc)	Ancaman	*Low*	2	0,0666
T3	Hackers (Intruders)	Ancaman	*Low*	2	0,0666
V2	Kesalahan SDM (Human Error)	Kelemahan	*High*	24	0,8
V3	Gangguan Perangkat Keras (Hardware Failure)	Kelemahan	*Medium*	15	0,5
V5	Kesalahan Pengiriman Data (Data Missing Recipient)	Kelemahan	*Low*	9	0,3
V6	Kesalahan Fungsional Perangkat Lunak (Software Bug)	Kelemahan	*High*	21	0,7
V7	Pembaharuan Aplikasi	Kelemahan	*Low*	5	0,1666
V8	Tidak ada kontrol pengawasan	Kelemahan	*Medium*	15	0,5
Total Kejadian	8	**Jumlah Rerata Probabilitas**		93	3,0998
Nilai Ancaman (NT)					0,3875

	ID Aset: SW-002
	Jumlah Hari: 30
	Nama Aset: Sistem Regristasi (Sireg)

Kejadian		Jenis	Probabilitas	Jumlah Kejadian Per 30 hari	Rerata Probabilitas
Kode	**Keterangan**				
T2	Serangan Virus (Virus Attack, Ex: Malware, Ransomware, Trojan, etc)	Ancaman	*Low*	0	0
T3	Hackers (Intruders)	Ancaman	*Low*	0	0
V2	Kesalahan SDM (Human Error)	Kelemahan	*High*	20	0,6666
V3	Gangguan Perangkat Keras (Hardware Failure)	Kelemahan	*Low*	5	0,1666
V5	Kesalahan Pengiriman Data (Data Missing Recipient)	Kelemahan	*Low*	0	0
V6	Kesalahan Fungsional Perangkat Lunak (Software Bug)	Kelemahan	*Low*	6	0,2
V7	Pembaharuan Aplikasi	Kelemahan	*Low*	1	0,0033
V8	Tidak ada kontrol pengawasan	Kelemahan	*Low*	1	0,0033
Total Kejadian	8	**Jumlah Rerata Probabilitas**		28	1,0398
Nilai Ancaman (NT)					0,1299

	ID Aset: SW-003
	Jumlah Hari: 30
	Nama Aset: Sistem informasi Pendaftaran Mahasiswa Baru (PMB)

Kejadian		Jenis	Probabilitas	Jumlah Kejadian Per 30 hari	Rerata Probabilitas
Kode	**Keterangan**				
T2	Serangan Virus (Virus Attack, Ex: Malware, Ransomware, Trojan, etc)	Ancaman	*Low*	0	0
T3	Hackers (Intruders)	Ancaman	*Low*	0	0
V2	Kesalahan SDM (Human Error)	Kelemahan	*High*	24	0,8
V3	Gangguan Perangkat Keras (Hardware Failure)	Kelemahan	*Low*	5	0,16

V5	Kesalahan Pengiriman Data (Data Missing Recipient)	Kelemahan	*Low*	0	0
V6	Kesalahan Fungsional Perangkat Lunak (Software Bug)	Kelemahan	*Low*	0	0
V7	Pembaharuan Aplikasi	Kelemahan	*Low*	1	0,0033
V8	Tidak ada kontrol pengawasan	Kelemahan	*Low*	0	0
Total Kejadian	8	**Jumlah Rerata Probabilitas**		30	0,9633
Nilai Ancaman (NT)					0,1204

	ID Aset: SDM-1				
	Jumlah Hari: 30				
	Nama Aset: Karyawan				
Kejadian		**Jenis**	**Probabilitas**	**Jumlah Kejadian Per 30 hari**	**Rerata Probabilitas**
Kode	**Keterangan**				
T1	Akses Ilegal (Unauthorized Access)	Ancaman	*Low*	9	0,3
T3	Hackers (Intruders)	Ancaman	*Low*	0	0
V3	Gangguan Perangkat Keras (Hardware Failure)	Kelemahan	*High*	24	0,8
V1	Kerusakan Data (Data Corruption)	Ancaman	*Low*	9	0,3
V2	Kesalahan SDM (Human Error)	Ancaman	*High*	25	0,8333
V5	Kesalahan Pengiriman Data (Data Missing Recipient)	Kelemahan	*Medium*	13	0,4333
V8	Tidak ada kontrol pengawasan	Kelemahan	*Low*	9	0,3
V10	Kurangnya tenaga ahli	Kelemahan	*Low*	9	0,3
Total Kejadian	8	**Jumlah Rerata Probabilitas**		98	3,2666
Nilai Ancaman (NT)					0,4

LAMPIRAN E
KUESIONER PENGUJIAN USER *ACCEPTANCE TEST*
PENELITIAN TUGAS AKHIR

KUESIONER PENELIATIAN TUGAS AKHIR

Nama : Daiyusman
Tempat : PTIPD
Waktu Pelaksaan : 15/7/2019
Jabatan : Jaringan

Pilih salah satu jawaban dari pertanyaan berikut ini yang Bapak/Ibu/Sdr/I anggap paling tepat dan berilah tanda silang (X) pada kotak yang tersedia.

A. Karakteristik Responden
Pengguna : (32) Umur
Jenis Kelamin : (✓) Laki-laki/ ( ) Perempuan

B. Kinerja Sistem Keamanan Informasi Penilaian Risiko menggunakan Metode NIST SP 800-30. Berikut ini pertanyaan-pertanyaan untuk mengetahui kinerja Sistem Keamanan Informasi Penilaian Risiko, anda cukup menilai sesuai kriteria berikut ini :
1. Sangat Tidak Setuju
2. Tidak Setuju
3. Netral
4. Setuju
5. Sangat Setuju

1) Informatif

No	Keterangan	1	2	3	4	5
1	Sistem yang ada menghasilkan informasi sesuai dengan target yang diharapkan					X
2	Informasi yang dihasilkan sesuai dengan proses yang terjadi					X
3	Sistem menyediakan informasi yang relevan				X	

2) Mudah Digunakan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada mudah diakses					X
2	Sistem yang ada mudah dipahami					X
3	Sistem yang ada mudah digunakan					X

4	Sistem yang ada mudah dipelajari				X	
5	Sistem memiliki proses input yang mudah				X	

3) Ketepatan Waktu

No	Keterangan	1	2	3	4	5
1	Sistem yang ada telah menyediakan informasi yang up to date				X	
2	Sistem yang ada mendukung penyediaan informasi untuk pengambilan keputusan yang cepat					X
3	Sistem yang ada selalu menyediakan laporan yang bersifat periodic secara tepat waktu					X
4	Sistem yang ada selalu memberikan informasi pada saat diperlukan				X	
5	Penyedia layanan informasi menyelesaikan sesuatu tepat pada waktunya			X		

4) Kehandalan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada selalu mudah untuk akses data yang diperlukan					X
2	Informasi yang diberikan dapat dipercaya					X
3	Layanan sistem informasi memberikan informasi yang handal				X	

TTD Narasumber,

(Putra Purdana, ST.)

KUESIONER PENELIATIAN TUGAS AKHIR

Nama : Riyan Perdana

Tempat : PKLD

Waktu Pelaksaan : 15-07-2019

Jabatan : Bagian aplikasi

Pilih salah satu jawaban dari pertanyaan berikut ini yang Bapak/Ibu/Sdr/I anggap paling tepat dan berilah tanda silang (X) pada kotak yang tersedia.

A. Karakteristik Responden
Pengguna : (38) Umur
Jenis Kelamin : (X) Laki-laki/ ( ) Perempuan

B. Kinerja Sistem Keamanan Informasi Penilaian Risiko menggunakan Metode NIST SP 800-30. Berikut ini pertanyaan-pertanyaan untuk mengetahui kinerja Sistem Keamanan Informasi Penilaian Risiko, anda cukup menilai sesuai kriteria berikut ini :
1. Sangat Tidak Setuju
2. Tidak Setuju
3. Netral
4. Setuju
5. Sangat Setuju

1) Informatif

No	Keterangan	1	2	3	4	5
1	Sistem yang ada menghasilkan informasi sesuai dengan target yang diharapkan					X
2	Informasi yang dihasilkan sesuai dengan proses yang terjadi				X	
3	Sistem menyediakan informasi yang relevan					X

2) Mudah Digunakan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada mudah diakses					X
2	Sistem yang ada mudah dipahami			X		
3	Sistem yang ada mudah digunakan				X	

4	Sistem yang ada mudah dipelajari				✓	
5	Sistem memiliki proses input yang mudah				✓	

3) Ketepatan Waktu

No	Keterangan	1	2	3	4	5
1	Sistem yang ada telah menyediakan informasi yang up to date			✓		
2	Sistem yang ada mendukung penyediaan informasi untuk pengambilan keputusan yang cepat				✓	
3	Sistem yang ada selalu menyediakan laporan yang bersifat periodic secara tepat waktu				✓	
4	Sistem yang ada selalu memberikan informasi pada saat diperlukan				✓	
5	Penyedia layanan informasi menyelesaikan sesuatu tepat pada waktunya				✓	

4) Kehandalan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada selalu mudah untuk akses data yang diperlukan				✓	
2	Informasi yang diberikan dapat dipercaya					✓
3	Layanan sistem informasi memberikan informasi yang handal			✓		

TTD Narasumber,

(RIVAYANTI, S.Kom)

KUESIONER PENELIATIAN TUGAS AKHIR

Nama : RIVA YANTI, S.Kom

Tempat : PTIPD

Waktu Pelaksaan : KAMIS, 15-07-2019

Jabatan : PRAKOM

Pilih salah satu jawaban dari pertanyaan berikut ini yang Bapak/Ibu/Sdr/I anggap paling tepat dan berilah tanda silang (X) pada kotak yang tersedia.

A. Karakteristik Responden
Pengguna : (42) Umur
Jenis Kelamin : ( ) Laki-laki/ (P) Perempuan

B. Kinerja Sistem Keamanan Informasi Penilaian Risiko menggunakan Metode NIST SP 800-30. Berikut ini pertanyaan-pertanyaan untuk mengetahui kinerja Sistem Keamanan Informasi Penilaian Risiko, anda cukup menilai sesuai kriteria berikut ini :
1. Sangat Tidak Setuju
2. Tidak Setuju
3. Netral
4. Setuju
5. Sangat Setuju

1) Informatif

No	Keterangan	1	2	3	4	5
1	Sistem yang ada menghasilkan informasi sesuai dengan target yang diharapkan				✓	
2	Informasi yang dihasilkan sesuai dengan proses yang terjadi				✓	
3	Sistem menyediakan informasi yang relevan				✓	

2) Mudah Digunakan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada mudah diakses				✓	
2	Sistem yang ada mudah dipahami				✓	
3	Sistem yang ada mudah digunakan				✓	

4	Sistem yang ada mudah dipelajari				X	
5	Sistem memiliki proses input yang mudah			X		

3) Ketepatan Waktu

No	Keterangan	1	2	3	4	5
1	Sistem yang ada telah menyediakan informasi yang up to date			X		
2	Sistem yang ada mendukung penyediaan informasi untuk pengambilan keputusan yang cepat				X	
3	Sistem yang ada selalu menyediakan laporan yang bersifat periodic secara tepat waktu				X	
4	Sistem yang ada selalu memberikan informasi pada saat diperlukan					X
5	Penyedia layanan informasi menyelesaikan sesuatu tepat pada waktunya					X

4) Kehandalan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada selalu mudah untuk akses data yang diperlukan				X	
2	Informasi yang diberikan dapat dipercaya					X
3	Layanan sistem informasi memberikan informasi yang handal					X

TTD Narasumber,

(INDRA MULIA SY)

KUESIONER PENELIATIAN TUGAS AKHIR

Nama : INDRA MULYA
Tempat : Divisi SERVER
Waktu Pelaksaan : 15/7/2019
Jabatan : sysadmin

Pilih salah satu jawaban dari pertanyaan berikut ini yang Bapak/Ibu/Sdr/I anggap paling tepat dan berilah tanda silang (X) pada kotak yang tersedia.

A. Karakteristik Responden
Pengguna : (38) Umur
Jenis Kelamin : (X) Laki-laki/ ( ) Perempuan

B. Kinerja Sistem Keamanan Informasi Penilaian Risiko menggunakan Metode NIST SP 800-30. Berikut ini pertanyaan-pertanyaan untuk mengetahui kinerja Sistem Keamanan Informasi Penilaian Risiko, anda cukup menilai sesuai kriteria berikut ini :
1. Sangat Tidak Setuju
2. Tidak Setuju
3. Netral
4. Setuju
5. Sangat Setuju

1) Informatif

No	Keterangan	1	2	3	4	5
1	Sistem yang ada menghasilkan informasi sesuai dengan target yang diharapkan				X	
2	Informasi yang dihasilkan sesuai dengan proses yang terjadi			X		
3	Sistem menyediakan informasi yang relevan			X		

2) Mudah Digunakan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada mudah diakses				X	
2	Sistem yang ada mudah dipahami					X
3	Sistem yang ada mudah digunakan				X	

4	Sistem yang ada mudah dipelajari					X
5	Sistem memiliki proses input yang mudah			X		

3) Ketepatan Waktu

No	Keterangan	1	2	3	4	5
1	Sistem yang ada telah menyediakan informasi yang up to date			X		
2	Sistem yang ada mendukung penyediaan informasi untuk pengambilan keputusan yang cepat					X
3	Sistem yang ada selalu menyediakan laporan yang bersifat periodic secara tepat waktu				X	
4	Sistem yang ada selalu memberikan informasi pada saat diperlukan					X
5	Penyedia layanan informasi menyelesaikan sesuatu tepat pada waktunya					X

4) Kehandalan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada selalu mudah untuk akses data yang diperlukan					X
2	Informasi yang diberikan dapat dipercaya				X	
3	Layanan sistem informasi memberikan informasi yang handal			X		

TTD Narasumber,

(.....)

KUESIONER PENELIATIAN TUGAS AKHIR

Nama : Tomi Z
Tempat : PTIPD.
Waktu Pelaksaan : 15/7/2019
Jabatan : Staff PTIPD.

Pilih salah satu jawaban dari pertanyaan berikut ini yang Bapak/Ibu/Sdr/I anggap paling tepat dan berilah tanda silang (X) pada kotak yang tersedia.

A. Karakteristik Responden
Pengguna : (32) Umur
Jenis Kelamin : (✓) Laki-laki/ ( ) Perempuan

B. Kinerja Sistem Keamanan Informasi Penilaian Risiko menggunakan Metode NIST SP 800-30. Berikut ini pertanyaan-pertanyaan untuk mengetahui kinerja Sistem Keamanan Informasi Penilaian Risiko, anda cukup menilai sesuai kriteria berikut ini :
1. Sangat Tidak Setuju
2. Tidak Setuju
3. Netral
4. Setuju
5. Sangat Setuju

1) Informatif

No	Keterangan	1	2	3	4	5
1	Sistem yang ada menghasilkan informasi sesuai dengan target yang diharapkan				X	
2	Informasi yang dihasilkan sesuai dengan proses yang terjadi					X
3	Sistem menyediakan informasi yang relevan			X		

2) Mudah Digunakan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada mudah diakses				X	
2	Sistem yang ada mudah dipahami			X		
3	Sistem yang ada mudah digunakan			X		

4	Sistem yang ada mudah dipelajari				X	
5	Sistem memiliki proses input yang mudah			X		

3) Ketepatan Waktu

No	Keterangan	1	2	3	4	5
1	Sistem yang ada telah menyediakan informasi yang up to date				X	
2	Sistem yang ada mendukung penyediaan informasi untuk pengambilan keputusan yang cepat				X	
3	Sistem yang ada selalu menyediakan laporan yang bersifat periodic secara tepat waktu			X		
4	Sistem yang ada selalu memberikan informasi pada saat diperlukan					X
5	Penyedia layanan informasi menyelesaikan sesuatu tepat pada waktunya					X

4) Kehandalan

No	Keterangan	1	2	3	4	5
1	Sistem yang ada selalu mudah untuk akses data yang diperlukan				X	
2	Informasi yang diberikan dapat dipercaya					X
3	Layanan sistem informasi memberikan informasi yang handal				X	

TTD Narasumber,

(Dr. Yusman.....)